Chris Mosby Ron Crumbaker Christopher W. Urban

MASTERING

Microsoft®

System Center Configuration Manager 2007 R2

Plan and Install SCCM 2007 R2

Monitor and Troubleshoot Client Systems



Mastering

System Center Configuration Manager 2007 R2

Mastering

System Center Configuration Manager 2007 R2

Chris Mosby
Ron Crumbaker
Christopher W. Urban



Acquisitions Editor: Agatha Kim Development Editor: Jim Compton Technical Editor: Jason Rutherford Production Editor: Rachel McConlogue

Copy Editors: Nancy Rapoport, Kim Wimpsett

Production Manager: Tim Tate

Vice President and Executive Group Publisher: Richard Swadley

Vice President and Publisher: Neil Edde Book Designers: Maureen Forys and Judy Fung

Proofreader: Publication Services, Inc.

Indexer: Ted Laux

Project Coordinator, Cover: Lynsey Stanford

Cover Designer: Ryan Sneed

Cover Image: © Pete Gardner / Digital Vision / Getty Images

Copyright © 2009 by Wiley Publishing, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-0-470-17367-1

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Library of Congress Cataloging-in-Publication Data is available from the publisher.

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *Mastering System Center Configuration Manager* 2007 R2. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at nedde@wiley.com, or if you think you've found a technical error in this book, please visit http://sybex.custhelp.com. Customer feedback is critical to our efforts at Sybex.

Best regards,

Neil Edde

Vice President and Publisher Sybex, an Imprint of Wiley

I would like to dedicate this book to my parents and my sister, for all of their love and support over the years.

To my brother Brian, I hope you found the peace that you didn't find in life. You are truly missed.

— Chris Mosby

I dedicate this book to my lovely and understanding wife, Martha, who stuck by me throughout this endeavor. I also want to dedicate this book to my three wonderful children — Nate, Abby, and Cole. Thank you for putting up with me while I was writing this book. I love you guys so much!

- Ron Crumbaker

To Ruthie, Noah and Livie — Daddy is home again! Thank you for your support through this project. It's back to head-to-head Xbox time rather than writing to all hours of the night; but Noah, I still cannot tell Mr. Gates you're a great Xbox tester when I visit Seattle. I think the policy at Microsoft is to hire testers older than eight years old.

— Christopher W. Urban

Acknowledgments

First and foremost, I would like to thank my wife Debbie for her infinite patience and understanding during the entire process of getting this book completed. I am truly a lucky man for having met her.

Next, I have to thank Ron Crumbaker, for coming on as an author when I was in desperate need of more help. His contribution to the book is greatly appreciated.

To Chris Urban, my first "partner in crime" in this endeavor, there were many times that he was the voice of reason when this project became chaotic.

To Rod Trent, of myITforum Inc., for getting me to start writing about SMS in the first place; without that encouragement, I doubt I would be where I am in life.

To the myITforum community, the absolute best and most supportive bunch of people on the planet; I hope I can repay in whatever way I can to all the help that they have given me over the years. This book is for you.

I would also like to thank the entire Configuration Manager product and writing team at Microsoft. Without their hard work and dedication, this book wouldn't even be possible.

Last and not least, I would like to thank the entire Sybex team, especially our Acquisitions Editor Agatha Kim. I am eternally grateful for their patience and sticking with us during all the setbacks that seemed to keep creeping up during the process of getting this book finished, even when things didn't look like they were going to work out.

— Chris Mosby

I want to thank the Microsoft Configuration Management team for giving us a great product to write about and for continually improving a great product. I also want to thank Agatha Kim at Wiley for giving me the opportunity to write this book. And thanks to Jim Compton for keeping me on track while writing it. Also, a huge thank you goes out to Chris Mosby for asking me to assist with this book.

As always, I want to thank my family for allowing me the time required for this book. And finally thanks to Jesus, my Lord and Savior, for saving me!

On a side note, I want to thank GM for bringing back the Camaro!

- Ron Crumbaker

I wanted to thank all of my family and friends who made this undertaking possible. Thanks to my father, Woody, who thought early on in my career I was giving him a snow job about receiving a technology grant for a school district to the tune of almost a million dollars. Dad, you should know I don't lie about money! Thanks to my mother, Jacque, who inspired me and gave me my spirit, undying drive, and endless pursuit for perfection. Last but most important, thanks to my wife, Ruthie; son, Noah; and daughter, Olivia; who gave me my opportunity to share knowledge and my passion with my friends and technical community abroad. Magic, I told you my technical "mumbo jumbo" would make it on the shelf before your trashy romance novel!

To the readers, I must thank you for your patience and understanding during a difficult period in my life. I feel it necessary to pass on a life story and how it may relate to you: This endeavor originally started out as a Configuration Manager 2007 book. As we wrote, we found ourselves in an interesting position to pull in the R2 components since they were released earlier than anticipated.

To some anxious readers who preordered this book, they were distraught. I assured some of my colleagues, friends, and customers that this would be a good thing.

Then life happened; in the beginning of 2008, I had a grand mal seizure while driving to a customer meeting in Indiana. Needless to say, everything was upside down for a while as I adjusted to life again. Thus, writing was put on the back burner as health took priority. I want to thank everyone who emailed me and sent me notes and instant messages wishing me well. Thanks to Martin Dey and Stephanie Toth for allowing me to attend MMS 2008 on their dime, just so I could "be" with the community; you'll never know how much it meant to me.

Thanks to Bill Anderson, Jeff Wettlaufer and the rest of the Configuration Manager product team for making our product the best as well as providing the Foreword to this book. Yes, I know, I owe you a dinner at MMS this year!

I must also thank the coauthors for their willingness to persevere and the Sybex family that never lost sight and endured this project to ensure it made it to print. Without friends, family, and community, this book could not have been completed. I am eternally grateful for you all enabling me to achieve one of my lifelong dreams.

— Christopher W. Urban

About The Authors

Chris Mosby started his career with SMS when he was a temporary employee with a subcontractor of the Department of Energy on the Hanford Nuclear Reservation. Chris, who had never even heard of SMS, was told "Here is the software and a server; make it work." After a few months of testing, his first SMS site went online in August of 1999, and he has been working with SMS and Configuration Manager ever since.

Chris is an active member of the 200,000-member myITforum (www.myitforum.com/), the premier site for the SMS and Configuration Manager community, since day one. He has written a handful of articles (www.myitforum.com/contrib/default.asp?cid=271) and posts several times a day to his myITforum blog about various topics such as security and patch management (http://myitforum.com/cs2/blogs/cmosby/default.aspx). In addition, Chris was awarded the Most Valuable Professional award in Configuration Manager from Microsoft, for the third time, for the period of April 2008 to June 2009.

Ron Crumbaker is the CTO of myITforum and is very active in the community space. Ron is currently a four-time MVP in the Microsoft System Center Configuration Manager area. Ron has written blogs, articles, and another book on various Microsoft topics. He has spoken at many Microsoft Management Summit conferences. In addition, Ron has three wonderful children, Nate, Abby, and Cole, as well as a lovely wife, Martha. Ron is very active in his church and is an ordained deacon and youth minister at his local church. Ron is a huge Camaro fan and is very excited to see the rerelease of the Camaro in 2010!

Christopher W. Urban is a management tools product specialist working within the Midwest district for Microsoft. He started his computer endeavors during high school while programming COBOL, RPG, and Basic. After serving in the United States Marine Corps, Christopher started his professional computer career in the public education sector doing technology integration.

In 1994, Christopher received his first Microsoft Certified Professional designation under Windows 3.51. Through the years, Christopher has attained various certifications and achievements such as MCSE, MCT, and MVP. Christopher was the founder of LearnSMS.com, which provided task-based, online video training, prior to joining Microsoft. In 2007, he was awarded the Management Insider Top Gun Award. Christopher currently runs the Microsoft Management track within the Chicago Windows User Group (http://portal.cwug.net).

Christopher resides in southern Wisconsin with his wife, Ruthie, of 11 years; his son, Noah; and his daughter, Olivia. When not working on technical information or solutions, he can be found gaming on Xbox, tinkering with home automation, or sport fencing.

Contents at a Glance

Foreword
Introduction
Chapter 1 • Overview of Operations Management
Chapter 2 • Planning a Configuration Manager Infrastructure
Chapter 3 • Interoperability with Systems Management Server 2003 45
Chapter 4 • Installation and Site Role Configuration
Chapter 5 • Client Installation
Chapter 6 • Software Distribution
Chapter 7 • Software Updates
Chapter 8 • Operating System Deployment
Chapter 9 • Asset Intelligence
Chapter 10 • Inventory and Software Metering
Chapter 11 • Reporting
Chapter 12 • Desired Configuration Management
Chapter 13 • Mobile Device Management
Chapter 14 • Network Access Protection
Chapter 15 • Troubleshooting
Chapter 16 • Disaster Recovery
Appendix • The Bottom Line 545
Index 567

Contents

Foreword	xx
Introduction	xxii
Chapter 1 • Overview of Operations Management	1
Understanding IT Service Management	
Exploring the IT Infrastructure Library	
Exploring the Microsoft Operations Framework	
Tying It All Together	
Defining Operations Management	
Systems Management	
Operations Management	15
Chapter 2 • Planning a Configuration Manager Infrastructure	1,
Configuration Manager Features	
What's New Since SMS 2003?	
What's New in Configuration Manager 2007 SP1?	
What's New in Configuration Manager 2007 St 1: What's New in Configuration Manager 2007 R2?	
Configuration Manager System Requirements	
Configuration Manager Client Requirements	
Configuration Manager Site Server Requirements	
Gathering Deployment Intelligence	
Determining What You Need to Accomplish	
Describing the Network	
Setting Up a Test Lab Environment	
Planning the Configuration Manager Deployment	
Active Directory Considerations	
Configuration Manager Site Boundaries	
Methods of Resource Discovery	
Configuration Manager Site Security	37
Configuration Manager Disaster Recovery	
Designing Your Configuration Manager Site	
Planning Configuration Manager Site Systems	
Planning the Configuration Manager Hierarchy	
Pilot Deployment: Determining How to Deploy Configuration Manager	
The Bottom Line	43
Chapter 3 • Interoperability with Systems Management Server 2003	
Interoperability with SMS 2003	
Interoperability Scenarios	46

Planning the Upgrade from SMS 2003 to Configuration Manager 2007	53
Identifying Configuration Change Requirements	
Setup / TestDBUpgrade	
Planning Your Upgrade Strategy	
Types of Upgrades	
Using the In-Place Upgrade Strategy	
Using the Side-by-Side Migration Strategy	
Using the Wipe and Load Strategy	
Upgrading the Administrator Console	
Post Upgrade or Installation Considerations	
The Bottom Line	
Chapter 4 • Installation and Site Role Configuration	67
Configuration Manager 2007 Site Types and Site Relationships	
Site System Roles	69
Site Server	69
Site Database Server	87
Site Server Roles	89
Installing and Configuring System Center Configuration Manager 2007 Service	
Pack 1	
Out-of-Band Management	
Asset Intelligence 1.5 Update	
Software Requirements	. 127
Implementing Configuration Manager 2007 Service Pack 1	127
Troubleshooting the Configuration Manager 2007 Service Pack 1 Installation .	128
Installing and Configuring System Center Configuration Manager 2007	
Release 2 (R2)	129
Client Status Reporting	. 129
Microsoft Application Virtualization Management	135
SQL Reporting Services	. 135
Operating System Deployment Improvements	137
The Bottom Line	139
Chapter 5 • Client Installation	1.41
Client Software Features	
Using Client Push Installation	
Configuring Boundaries	
Creating the Client Push Installation Account	
Configuring Discovery Methods	
Configuring Client Push Settings	
Performing an Attended Client Push	
Other Automatic Installation Methods	
Logon Script Installation	
Imaging	
Manually Installing the Client	
Verifying Client Installation	159 161
The Bottom Line	161

Chapter 6 • Software Distribution	163
What's New in Software Distribution	163
Prerequisites for Software Distribution	165
Internal Dependencies	165
Distribution Point Requirements	
Elements of Software Distribution	167
The Advertised Programs Client Agent	167
Packages	
Programs	
Distribution Points	170
Advertisements	171
Collections	
Preparing for Software Distribution	
The Software Distribution Process	
Creating Collections	176
Creating Packages	
Creating Programs	
Configuring Distribution Points	
Creating Advertisements	
Monitoring Software Distribution Status	
Using Software Distribution Reports	
Using the Status Message Viewer	
Using Log Files	
Virtual Application Packages	
Virtual Application Package Terminology	
Importing a New Virtual Application Package	
Configuring Configuration Manager Clients to Run Virtual	
Applications	233
Configuring Virtual Application Package Streaming	233
Advertising a Virtual Application Package	
The Bottom Line	234
Chapter 7 • Software Updates	237
What's New in Software Updates	237
Prerequisites for Software Updates	
Elements of Software Updates	
Software Update Point	
Software Updates Client Agent	
Software Updates Metadata	
Software Update Files	
Software Update Objects	
Update Lists	
Deployment Templates	
Deployment Packages	
Deployments	
System Center Update Publisher	

The Software Update Process in Configuration Manager	. 244
Synchronization	
Compliance	. 247
Deployment	. 247
Planning to Use Software Updates in Configuration Manager	. 249
Determine What Needs to Be Accomplished with Software Updates	. 249
Determine What Is on the Network Now and What Has Been Used in the Past.	. 258
Test in an Isolated Lab	. 261
Configuring Software Updates	. 262
Configuring the Software Updates Client Agent	. 262
Installing Windows Server Update Services 3.0 Server	. 264
Installing the Windows Server Update Services 3.0 Administration Console	. 267
Setting Up the Active Software Update Point	. 269
Configuring Software Updates Settings and Synchronization	. 275
Synchronizing Updates with Export and Import	
Supporting Software Updates for SMS 2003 Clients	. 280
Preparing Software Updates for Deployment	. 285
Finding the Software Updates to Be Deployed	. 285
Downloading Software Updates	. 290
Creating an Update List	. 295
Creating Deployment Templates	. 298
Deploying Software Updates with the Deploy Software Updates Wizard	. 303
Monitoring Software Update Deployments	. 306
The Bottom Line	. 307
Chapter 8 • Operating System Deployment	309
Preparing Configuration Manager 2007 for OSD	
Setting Up the User State Migration Tool	. 309
Configuring the Network Access Account	
	. 310
Creating the Configuration Manager Client Install Package	. 310 . 310
Creating a USMT Package	. 310 . 310 . 312
Creating a USMT Package	. 310 . 310 . 312 . 315
Creating a USMT Package	. 310 . 310 . 312 . 315 . 316
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image	. 310 . 312 . 315 . 316 . 317
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer	. 310 . 312 . 315 . 316 . 317 . 319
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image	. 310 . 312 . 315 . 316 . 317 . 319
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image	. 310 . 312 . 315 . 316 . 317 . 319 . 322
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image Developing a Task Sequence for Deployment	. 310 . 312 . 315 . 316 . 317 . 319 . 322 . 323
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image Developing a Task Sequence for Deployment Advertising the Task Sequence	. 310 . 312 . 315 . 316 . 317 . 319 . 322 . 323 . 324
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image Developing a Task Sequence for Deployment	. 310 . 312 . 315 . 316 . 317 . 319 . 322 . 323 . 324
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image Developing a Task Sequence for Deployment Advertising the Task Sequence Deploying the Operating System on "Bare Metal" Creating PXE Service Points	. 310 . 312 . 315 . 316 . 317 . 319 . 322 . 323 . 324 . 328 . 331
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image Developing a Task Sequence for Deployment Advertising the Task Sequence Deploying the Operating System on "Bare Metal" Creating PXE Service Points Setting Up a Computer Association	. 310 . 312 . 315 . 316 . 317 . 319 . 322 . 323 . 324 . 331 . 331
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image Developing a Task Sequence for Deployment Advertising the Task Sequence Deploying the Operating System on "Bare Metal" Creating PXE Service Points Setting Up a Computer Association Creating a Task Sequence for the Bare-Metal OSD	. 310 . 312 . 315 . 316 . 317 . 319 . 322 . 323 . 324 . 331 . 331 . 334 . 339
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image Developing a Task Sequence for Deployment Advertising the Task Sequence. Deploying the Operating System on "Bare Metal" Creating PXE Service Points Setting Up a Computer Association Creating a Task Sequence for the Bare-Metal OSD Advertising the Bare-Metal Task Sequence	. 310 . 312 . 315 . 316 . 317 . 319 . 322 . 323 . 324 . 328 . 331 . 331 . 334 . 339 . 343
Creating a USMT Package Configuring the State Migration Point Role Distributing the Boot Image Package Developing a Task Sequence for Creating a Capture Image Creating an Image of a Reference Computer Packaging and Advertising the Image Distributing and Deploying the Image Developing a Task Sequence for Deployment Advertising the Task Sequence Deploying the Operating System on "Bare Metal" Creating PXE Service Points Setting Up a Computer Association Creating a Task Sequence for the Bare-Metal OSD	. 310 . 312 . 315 . 316 . 317 . 319 . 322 . 323 . 324 . 328 . 331 . 331 . 334 . 339 . 343

Chapter 9 • Asset Intelligence	. 349
What's New in Asset Intelligence in Configuration Manager	. 349
Requirements for Asset Intelligence	. 350
Client Agent Prerequisites	. 350
Hardware Inventory File Modification Requirements	. 351
Site Maintenance Task Requirements	. 352
Windows Event Log Settings	. 352
Elements of Asset Intelligence	. 352
Asset Intelligence Catalog	. 352
Asset Intelligence Validation States	. 355
Asset Intelligence Synchronization Point	. 355
The Asset Intelligence Home Page	. 356
Asset Intelligence Reports	. 358
Configuring Asset Intelligence	. 362
Enabling Asset Intelligence	. 362
Configuring Collecting Client Access License Data	. 363
The Bottom Line	
Chapter 10 • Inventory and Software Metering	. 369
Inventory in Configuration Manager 2007	. 369
Collecting Hardware Inventory	
Collecting Software Inventory	. 374
Using Resource Explorer to View Inventory	
Scheduling Inventory	. 377
Configuring Inventory	
Configuring Software Inventory for a Configuration Manager Site	. 387
Troubleshooting Inventory	
Software Metering in Configuration Manager 2007	. 393
What's New in Software Metering for Configuration Manager 2007	. 393
Overview of Software Metering	
Configuring Software Metering	. 394
The Bottom Line	
Chapter 11 • Reporting	. 401
Setting Up Reporting Point Roles	. 401
Installation of the Reporting Point Role	
Viewing the New Virtual Web Directory in IIS	
Default Reports	
Viewing Available Reports	. 410
Running a Report	
Running a Report from the Administrator Console	
Running a Report from the Report Viewer	
Choosing a Technique	
Creating and Managing Reports	
Creating a New Report from the Console	
Cloning a Report	

Importing and Exporting Reports	. 417
Creating and Managing Security on Reports	
Basic SQL Commands	
Creating Dashboards	
The Bottom Line	. 424
Chapter 12 • Desired Configuration Management	425
Overview of Desired Configuration Management	. 425
What Can You Do with Desired Configuration Management?	
Configuration Items	
Configuring Desired Configuration Management Client Agent Settings	
Creating Configuration Items	
Name, Description, and Category	
Choosing a Detection Method	
Creating and Validating an Object	
Parent and Child Configuration Items	
Building a Configuration Baseline	. 449
Creating the Initial Baseline	
Add CIs to the Configuration Baseline	
Assigning the Configuration Baseline to Clients	
Additional Configuration Baseline Options	
Desired Configuration Management Reporting	
The Bottom Line	. 457
Chapter 13 • Mobile Device Management	. 459
Setting Up a Mobile Device Management Point	
Enabling Distribution Points for Supporting Mobile Devices	
Configuring the Mobile Device Client Agent	
Extending Inventory on Client Desktop Computers	
Setting Up the Device Management Inventory Extension Package	
Specifying a Distribution Point for the Package	
Advertising the Package to Clients	
Installing the Client Software on a Mobile Device	
Editing the Device Client Deployment File	
Deploying the Device Client Installer to Clients	
Verifying Client Installation on Mobile Devices	
Verifying Using Collection Membership	. 474
Verifying Using Log Files	. 474
Verifying Installation on the Mobile Device	. 475
Using Reports to Verify Installation	. 475
Deploying Software to Mobile Clients	
Using Reports to Verify Mobile Client Health	. 479
The Bottom Line	

Chapter 14 • Network Access Protection	. 481
Introducing Network Access Protection (NAP)	481
Requirements for Implementing NAP on Your Network	
A Quick Look at the NAP Architecture in the Operating System	
Exploring the NAP Enforcement Methods	
802.1x NAP (Wired or Wireless)	484
DHCP NAP	
VPN NAP	486
IPsec NAP	487
Preparing for NAP and Configuration Manager 2007 Integration	
Configuring Configuration Manager and NAP	488
Phasing NAP into a Configuration Manager 2007 Environment	491
802.1x (Wired or Wireless) NAP with Configuration Manager 2007	494
DHCP NAP with Configuration Manager 2007	495
VPN NAP with Configuration Manager 2007	496
IPsec NAP with Configuration Manager 2007	497
The Bottom Line	500
Chapter 15 • Troubleshooting	. 501
Creating the Maintenance Plan	
Using Troubleshooting Tools	
Log Files	
Status Messages	
Troubleshooting Configuration Manager Deployment	
Troubleshooting the Configuration Manager Console	517
Troubleshooting Clients with the Client Status Tool	518
Client Status Reporting	
Client Status Reporting Prerequisites	
Installing and Configuring Client Status Reporting	
Importing and Viewing the Client Status Reports	
The Bottom Line	
The Bottom Ellie	. 022
Chapter 16 • Disaster Recovery	F22
Planning for Disaster Recovery	
Backing Up Configuration Manager	
Backup Considerations for the Central Site	
Copying Site Backups to Another Location	
Archiving the Backup Snapshot to Another Server with AfterBackup.bat	
Configuring the Backup ConfigMgr Site Server Maintenance Task	
Understanding the Effects of a Site Failure	
The Site Repair Wizard	
The Hierarchy Maintenance Tool (Preinst eye)	

Recovering Configuration Manager How to Start the Site Repair Wizard Recovering a Central Site Recovering a Primary Site Performing a Site Reset After Recovery Post-Site-Repair Tasks	. 532 . 533 . 537 . 538 . 538
The Hierarchy Maintenance Tool (Preinst.exe)	
The Bottom Line	. 543
Appendix • The Bottom Line	545
Chapter 2: Planning a Configuration Manager Infrastructure	. 545
Chapter 3: Inoperability with Systems Management Server 2003	. 545
Chapter 4: Installation and Site Role Configuration	. 547
Chapter 5: Client Installation	. 551
Chapter 6: Software Distribution	
Chapter 7: Software Updates	
Chapter 8: Operating System Deployment	. 556
Chapter 9: Asset Intelligence	. 557
Chapter 10: Inventory and Software Metering	. 558
Chapter 11: Reporting	
Chapter 12: Desired Configuration Management	
Chapter 13: Mobile Device Management	
Chapter 14: Network Access Protection	
Chapter 15: Troubleshooting	. 565
Chapter 16: Disaster Recovery	. 566
Index	567

Foreword

To all of our customers . . .

Wow — it's been almost 14 years now since the announcement was made for this new product from Microsoft: Microsoft Systems Management Server (SMS) 1.0. The original charter was to "provide easier and more cost-effective management of desktop hardware and software throughout large-scale computing systems, easing what has been one of the most expensive and time-consuming aspects of client-server computing and enabling customers to run their businesses more effectively." To do this, SMS 1.0 boasted features such as hardware and software inventory, software distribution and installation, performance monitoring and analysis, and troubleshooting. It's safe to say that, although that charter and those features still resonate with our customers today, the characteristics and importance of those features has taken on new and different meanings over the past 14 years, and we are so proud of what we think System Center Configuration Manager 2007 adds to this long history in helping solve those needs. Quite frankly, this is the most significant release of SMS/SCCM ever, and the value we believe it will bring to you is tremendous. Fourteen years ago, no one thought about "patch Tuesday," and being quarantined involved a doctor. Deploying Windows wasn't as hard — you just put in the six floppy disks! Sarbanes-Oxley and HIPAA were just part of the "golden rule," not governmental and corporate obligations. The core disciplines have remained the same, but the world has evolved to place further demands on those cores. That was what SCCM 2007 was all about: continuing to solidify and extend that core discipline of change and configuration management to today's business problems, with the reliability you've come to expect.

But the greatest thing in those 14 years is not the 1s and 0s we've shipped to the market; it's the relationships we've made with you, the tens of thousands of SCCM administrators around the world. We are very aware that a large degree of the SMS/SCCM success over the years is attributable to this community of administrators who have shared a unique spirit for "the unsolvable problem" of systems management. What we've built, you've tweaked. What we've omitted, you've filled in. What we've gotten wrong, you've worked around — and let us know how to do it right next time. It's this relationship in working with you to build our software and solve your needs that makes us most proud to come to work every day.

What we've all learned in the software industry is that software is never perfect. We obviously continue to strive for perfection when it comes to quality and security, but we know with as large and as diverse a group of customers that we have, there will be no way we get every feature you need or every feature done in the way you need it. However, our "luxury" is that we have the *best* people on the planet using our product on a daily basis. You — our SCCM administrators — share the same passion in solving your problems and helping your fellow administrators that we do in building the product. This book is just another testament to that dedication and spirit. We want to thank the authors (SCCM administrators, like you) for their ongoing support of our product and this community. And, we look forward to continuing this relationship for years (and releases) to come!

With greatest admiration, The System Center Configuration Manager Product Group

Introduction

Microsoft has accomplished a lot to make System Center Configuration Manager 2007 the product that it is today. Starting as a little known niche product, back when there wasn't even really a name for what it did, it's now the premier configuration management product on the market.

This book is written by a group of individuals who have been through the growing pains of this product, some even from day one, and who have even helped Microsoft improve what is now Configuration Manager by countless hours of real-world use and testing.

Welcome to *Mastering System Center Configuration Manager 2007 R2*. We all hope that you find this book helpful in learning how to use Configuration Manager to its full potential.

The Mastering Series

The Mastering series from Sybex provides outstanding instruction for readers with intermediate and advanced skills in the form of top-notch training and development for those already working in their field and provides clear, serious education for those aspiring to become pros. Every Mastering book includes the following:

- Real-world scenarios, ranging from case studies to interviews that show how the tool, technique, or knowledge presented is applied in actual practice
- Skill-based instruction, with chapters organized around real tasks rather than abstract concepts or subjects
- Self-review questions, so you can be certain you're equipped to do the job right

What This Book Covers

Mastering System Center Configuration Manager 2007 R2 covers Microsoft's System Center Configuration Manager 2007 R2 (which requires that SP1 be installed). We will detail the changes to Configuration Manager since its initial release and the new features that were introduced in both SP1 and R2.

These new features include but are not limited to:

- The new Software Updates system, which has been completely redesigned from SMS 2003 and is based on Windows Update Services technology
- ◆ A completely new system for Operating System Deployment
- An improved system of Software Metering
- Enhanced Asset Intelligence for asset tracking

- SQL Reporting Services in Configuration Manager 2007 R2
- Improved Software Distribution with network bandwidth enhancements

What You Need to Get the Most Out of This Book

To be able to follow the step-by-step instructions in this book, it is recommended that you have a minimum of Windows Server 2003 R2 SP1 and SQL Server 2005 SP2 installed, with all the applicable updates. Also, having the media for Configuration Manager 2007 RTM, SP1, and R2 is a plus, because we will go through installing this software in the first few chapters. Your computer also needs an Internet connection so you can download updates in various parts of the installation process. Evaluation versions of any of this software are fine for our purposes.

How We Structured This Book

To help you understand the features of Configuration Manager, we have structured this book to match the names of features as they are listed in the Configuration Manager administration console wherever possible, with a few exceptions.

Chapter 1, "Overview of Operations Management," covers general management concepts, such as ITIL and MOF, and how System Center Configuration Manager 2007 R2 supports those concepts.

Chapter 2, "Planning a Configuration Manager Infrastructure," covers Site Roles, how they are leveraged and application of them in your enterprise.

Chapter 3, "Interoperability with Systems Management Server 2003," addresses current SMS 2003 customers needs in coexistence as well as migration strategies.

Chapter 4, "Installation and Site Role Configuration," covers the details of Site Role installation, configurations, and troubleshooting.

Chapter 5, "Client Installation," covers Client Installation aspects in relation to Configuration Manager 2007 like the various installation methods found within Configuration Manager 2007.

Chapter 6, "Software Distribution," gives a comprehensive look at planning, configuring, and using Software Distribution elements like the Advertised Programs Client agent, Collections, Packages, and Programs.

Chapter 7, "Software Updates," gives you a step-by-step guide on this completely redesigned feature that is now based on Windows Update Services.

Chapter 8, "Operating System Deployment," gives you an in-depth look at how Configuration Manager 2007 allows an administrator the ability to deploy a single Operating System to multiple types of machines.

Chapter 9, "Asset Intelligence," covers the updated information knowledge base that was carried over from Asset Management that was introduced in SMS 2003 SP 3 and gives you even more tools to help keep track of your hardware and software assets.

Chapter 10, "Inventory and Software Metering," is the heart of Configuration Management Server 2007, one of the core features that most other features tie in to work.

Chapter 11, "Reporting," is probably the most used aspect of Configuration Manager by users outside the IT Department. It gives other users the ability to report on various parts of Configuration Manager.

Chapter 12, "Desired Configuration Management," offers an in-depth look at setting up a predefined level of standards for all your devices and how Configuration Manager 2007 will ensure your clients are maintained at that standard.

Chapter 13, "Mobile Device Management," gives you an inside look at Mobile Devices and how Configuration Manager 2007 can manage these types of devices.

Chapter 14, "Network Access Protection," gives information on how to use NAP with Configuration Manager 2007 to help maintain a healthy and secure network.

Chapter 15, "Troubleshooting," gives a base on how to ensure your Configuration Manager 2007 environment stays healthy and gives you a baseline of where and what to look for if problems arise.

Chapter 16, "Disaster Recovery," gives the information necessary to protect your Configuration Manager databases by backing them up properly so that you can use those backups to recover from a disaster if it strikes.

Errata

We have done our best to make sure that the content in this book is as accurate as possible at the time it was written. If you discover any mistakes that we have missed in the editing process, please let us know at http://sybex.custhelp.com so we can address them in future versions of this book.

Mastering

System Center Configuration Manager 2007 R2

Chapter 1

Overview of Operations Management

Before we delve into the technology at hand, the System Center Configuration Manager product, it's important to define what operations management is, what it defines, and why we need it. As an IT manager, you are not responsible for certain key business activities. When those activities are being processed on your servers, however, you become a critical piece of the puzzle in overall IT systems management. You may control the SQL servers, but they house information that is critical to day-to-day operation of the Billing department, for example. Suddenly, you start to see how everything ties together. A missing or damaged link in the chain, or an unplanned removal of the chain, may cause much more damage than you originally thought.

This is just one of the many reasons Microsoft created the Microsoft Operations Framework (MOF), which is based on the IT Infrastructure Library (ITIL). The idea behind MOF and ITIL is to create a complete team structure with the ultimate goal of service excellence. Numerous groups fall under the IT Department tag, but we often see many of them acting as separate departments rather than as one cohesive unit. Desktop support, application developers, server support, storage administrators, and so forth are all members of IT, but they are not always as unified as they should be.

System Center Configuration Manager 2007 was built with MOF and the ITIL in mind, so we will start the book by describing both for background. But SCCM is much more than just a mechanism to deploy software. In this chapter, you learn how we define IT service management, how ITIL is the foundation, and how MOF expands ITIL, but you will also learn about the Dynamic Systems Initiative and all of the Microsoft System Center products.

Understanding IT Service Management

ITIL and MOF were introduced as a way to deliver consistent IT Service Management (ITSM). Some of the key objectives of ITSM are:

- To align IT services with current and future needs of the business and its customers
- ◆ To improve the quality of IT services delivered
- ◆ To reduce the long-term cost of service provisioning

Think of ITSM as a conduit between the business and the technology that helps run the business. Without a proper conduit in place, one cannot function properly without the other. ITSM is about process, *not* about software products.

Exploring the IT Infrastructure Library

Before we dig into the inner workings of ITIL Version 2, it is important for the ITIL beginner to understand that ITIL, and its counterpart Microsoft Operations Framework (MOF) Version 3, are not based on technology. Both ITIL and MOF are based on IT processes. This is important to understand before proceeding. Readers interested in IT processes and procedures, as well as how the Microsoft System Center family of products fits into these processes, should find the rest of this chapter very interesting. For those of you who yawned and rolled your eyes, we'll meet you back at Chapter 2.

If you start researching ITIL, you will find that it is a series of books that describe an approach to IT service management. Originally created in the United Kingdom to address strict operations management standards, ITIL has become the accepted standard in IT service management. The library is owned by the UK government's Office of Government Commerce (OGC). If you really want to get cozy with ITIL, be prepared to spend a lot of time reading. In its original form, the ITIL volumes were at a count of 60 books. These books were created by industry leaders of the time and described best practices for IT processes.

There is much more to ITIL than just the books, however. ITIL as a whole includes the books, certification, ITIL consultants and services, and ITIL-based training and user groups. ITIL is mainly updated by its own user group, known as the IT Service Management Forum (itSMF). The last piece of the puzzle, ITIL certification, is administered by the Netherlands Examination Institute for IT (EXIN) and the Information Systems Examination Board (ISEB).

ITIL can be divided into two categories: Service Support and Service Delivery. The two categories include numerous processes. Service Support is described as the practice of disciplines that enable IT Services to be provided. Without those disciplines, which we'll outline shortly, any attempt to provide IT Services would potentially be unmanaged and possibly chaotic. Underlying this division is the difference between what is considered a *user* of the system and what is considered a *customer* of the system.

Now you may be thinking, "I run an internal network. Everyone on my network is a user; we don't have any customers who connect into the network." In all actuality, every administrator (admin) has both users and customers on their network, and often the same individual can be both a user and a customer. For example, HallieM is a *user* of the network when she interacts with the Service Desk. HallieM is also a *customer* of the network when she obtains certain services from another department, such as services that she must pay for or services that have Availability Management in place, as would be the case with e-mail and database services. Table 1.1 shows the breakdown of the difference between service support and service delivery.

SERVICE DESK

We will first look at the Service Desk, as it is unique among the items in Table 1.1. The Service Desk is a *function*, unlike the other items listed, which are processes. All incident reporting and service requests are routed through the Service Desk. It is the function that ties the service providers with the users, keeping users informed of service events and actions that may impact their day-to-day activities. The Service Desk becomes a single point of contact for customers and users to interact with the IT department. This approach helps expedite the call process by managing it in a timely and satisfactory way.

INCIDENT MANAGEMENT

Incident Management is the mechanism by which the Service Desk records, updates and tracks the enterprise "fires." The Incident Management process is mainly concerned with restoring normal

CATEGORY	Focus	Areas
Service Support	User Focused	Incident Management Problem Management Configuration Management Change Management Release Management
Service Delivery	Customer Focused	Service-level Management Financial Management Availability Management Capacity Management Service Continuity Management

TABLE 1.1: ITIL Service Support and Service Delivery Differences

service operations as soon as possible. This will help minimize any adverse effects on business operations and will ensure high levels of service quality and availability. Service-Level Agreements (SLAs) will determine what a "normal" service operation is. Information is collected about the incident to allow changes or enhancements in the environment to prevent future incidents. This information can also be used to compare against SLA compliance metrics and service quality information.

PROBLEM MANAGEMENT

The Problem Management process is mainly concerned with minimizing the impact of incidents and problems. The goal is to reduce incident resolution times by providing insights for known errors and removing the underlying causes. This strategy improves IT service quality by helping the Service Desk resolve incidents at the time of logging. If an incident can be resolved at the time of logging, business impact is reduced, business efficiency is improved, and IT efficiency is improved.

The problem-management process should not only be considered a "reactive" approach, however. When dealing with Incident Management, problem control, or error control, it is very reactive. The problem-management process can be viewed as "proactive" when you consider how it is used for problem prevention.

Problem investigation and diagnosis are used when known errors are created. During this investigation and diagnosis time, insight details of the known errors are distributed until a fix for the problem is found. This approach helps with the staffing of the incident-management process, thus ensuring there aren't too many IT staff members duplicating work while trying to fix the same issue.

CONFIGURATION MANAGEMENT

The Configuration Management process is responsible for keeping an accurate and up-to-date model of the entire IT infrastructure. It uses this information to help support a number of areas by doing the following:

- Allowing for assessment of Change or Problem Management functions
- Allowing financial information to be gathered to help determine lease, rental, maintenance, and support costs for IT infrastructure components

- Supplying information about component performance and reliability to support capacity and Availability Management
- Improving security by identifying the location and details of assets, making it difficult for unauthorized changes to be carried out undetected
- Helping with legal obligations by identifying the location of unauthorized software, determined by enabling authenticity checks on software and making sure current, correct versions of the software are being used

Configuration Management uses this information to identify relationships between items that are going to be changed and any other components of the infrastructure that an item is tied to. Such a strategy enables the owners of the other components to be notified and involved in the impact-assessment process.

CHANGE MANAGEMENT

The Change Management process is used to ensure that standard methods are used when implementing change, and for developing and documenting reusable processes. Implementing a change management system can reduce the possibility that a change in the environment could cause a failure, thus resulting in an incident.

The IT infrastructure is constantly changing. Patches, service packs, updates, bios updates, and so forth are released on an almost daily basis. Having a safe and repeatable process in place is vital to service management.

RELEASE MANAGEMENT

Changes in the environment often result in the need for new versions of software, new hardware, new documentation, and so forth. The Release Management process works closely with Change Management and Configuration Management to produce a secure and managed rollout of the new item. Consequently, physical changes to the environment are taken into account and the transition to live operation is successful — including both hardware and software releases.

The quality of a new version of software is tested in this process, along with tests to determine whether patches and updates are going to affect a piece of "approved" software. In this way, the process guarantees that only the authorized versions of software releases are being installed.

SERVICE LEVEL MANAGEMENT

The Service Level Management (SLM) process is responsible for creating SLAs and making sure Operation Level Agreements (OLAs) are met at all times. During this process, changes to the environment are assessed to determine the effect on SLAs.

SLAs play an important role in SLM. They help set expectations for IT by determining what the customer's service-level requirements are, and they help customers by having a measurable understanding of what "good" service is. Both sides can agree on timelines for deliverables for everything from service upgrades to updates, to incident resolution. SLAs also provide a clear understanding of what value customers are receiving from IT and can be used as a basis for charging for IT services. This brings us to the Financial Management process.

FINANCIAL MANAGEMENT

The Financial Management process is responsible for determining the costs of IT services as well as calculating the return on IT service investments. It is also a key in the role of recovering costs

from customers if you charge for your services. As mentioned earlier, having SLAs in place to manage expectations is very important.

Budgeting can become much more accurate as well because Financial Management is responsible for tracking costs of IT assets and resources. Financial management allows you to break down the money spent on IT services so you can clearly view where IT budget money went. Due to budgeting being more accurate and a much more precise data point, it helps support future business decisions on IT investments.

If you are considering charging for IT services, a fair recovery system is determined by data gathered through the financial-management process. Charging for internal services has its advantages and disadvantages. One advantage to charging for IT services is that it helps customers and users see the value of IT. Customers and users may also behave differently if they are faced with a "charging" model. Such a model helps the customers decide whether the services they are receiving are cost-justified. Using a model could lower the demands on the IT department.

One of the disadvantages of charging for services is that the customer has the ability to take business or services elsewhere, which could have a severe effect on budgeting. Also, charging systems are often expensive, and the cost of such a model could offset the money that is generated by the system.

CAPACITY MANAGEMENT

The Capacity Management process involves determining the required service delivery, the current service delivery, and the IT infrastructure, and ensuring that all current and future capacity and performance requirements from the business are met. Capacity management also needs to take into account changes in new technology and the improvement in performance that new technology brings to the table. Basically, this process is responsible for identifying the current service delivery as well as the service delivery potential at any given time.

Capacity management is responsible for making sure business requirements for system capacity are met at all times. Again, this does not directly relate to a technical capacity. It is related to the business requirements for the system, not necessarily the performance of the system.

IT SERVICE CONTINUITY MANAGEMENT

The IT Service Continuity Management process ensures that an organization can continue to function with predetermined and agreed-on levels of IT services to support the minimum business requirements following an interruption to the business. The idea behind this process is that the organization will always have a base level of IT services that are required at all times.

Each IT service is examined to determine the minimum level it can function at to meet the business requirements. A plan is then put in place to guarantee that this level of service can be reached at all times under any circumstances.

AVAILABILITY MANAGEMENT

The Availability Management process deals with the design, implementation, and management of IT services to guarantee that certain business requirements for availability are obtained. This requires information from both Incident Management and Problem Management to determine why an IT service failed and the time it took to resume service. This process can help IT departments meet SLAs that define availability levels. These SLAs cannot be met without a thorough understanding of the availability and reliability of IT components.

Availability Management is a very high-profile process. Take an accounting server offline during a month-end run and see what kind of attention it gets. Because of this high-profile status,

it is beneficial to have a single process owner for all availability issues to ensure that consistent and comprehensive measures are taken for managing and improving availability to IT systems.

Exploring the Microsoft Operations Framework

As stated earlier, the Microsoft Operations Framework (MOF) is the basis of System Center Configuration Manager 2007. The MOF was developed by Microsoft and a group of partners to expand on the best practices developed by ITIL. MOF includes a plethora of resources that are available to help you achieve mission-critical system reliability, manageability, supportability, and availability with Microsoft products and technologies. These resources are in the form of white papers, operations guides, assessment tools, best practices, case studies, templates, support tools, courseware, and services. All of these resources are available on the official MOF website at www.microsoft.com/mof.

HOW MOF EXPANDS ITIL

While ITIL is based on IT operations as a whole, MOF has taken the route of providing a service solution as its core. MOF focuses on the release and life cycle of a service solution, such as an application or infrastructure deployment.

Because ITIL was based on a philosophy of "adopt and adapt," Microsoft leveraged that strategic fundamental basis for the MOF. Although Microsoft supports ITIL from a process perspective, Microsoft decided to make a few changes and add a few things when it built MOF. One of these changes and additions includes moving to a "prescriptive" process model. Microsoft defines the ITIL process model as "descriptive." It has more of a "why" approach, whereas MOF has more of a "prescriptive," or "how," approach.

MOF also introduced the concept of Service Management Functions (SMFs). As Table 1.2 illustrates, there are now 21 SMFs that describe the series of management functions performed in an IT environment. All of these SMFs map to an ITIL-based best practice for performing each function. Notice that the SMFs are grouped into *quadrants*, a concept we explain in the section "The Microsoft Operations Framework Process Model" shortly.

MOF also extended many of the existing processes in ITIL and created new processes. These will be discussed later in the chapter.

MOF also introduced the Team model. This gives the MOF two core models; the Team and Process models. The Team model was added to fill a gap in ITIL, which identifies roles for the process owner of each operation process, whereas MOF creates seven distinct role clusters that describe the functional role or team:

Service Primary responsibility is to make sure all IT services are at a satisfactory level to customers and users. This is done by creating SLAs and ensuring that they are being met on a regular basis.

Infrastructure Responsible for ensuring that plans are in place to keep networking, telecommunications, hardware, and software running in order to satisfy business requirements.

Support Maps to the Service Desk, Incident Management, and Problem Management functions in ITIL.

Operations Responsible for making sure that the day-to-day tasks of running the IT systems are met, according to SLAs.

Partner This is more of a "virtual" team in the IT department, usually made up of outsource vendors, IT partners, resellers, service providers, consultants, and so forth.

TABLE 1.2:	MOF Quadrants	Breakdown	
QUADRANT			SMF
Optimizing			Service Level Management Financial Management Services Continuity Management Availability Management Capacity Management Workforce Management
Changing			Change Management Configuration Management Release Management
Operating			System Administration Security Administration Service Monitoring and Control Job Scheduling Network Administration Directory Services Administration Print and Output Management Storage Management
Supporting			Service Desk Incident Management Problem Management

Security Responsible for data confidentiality, data integrity, and data availability.

Release Transitions a release between development or test environments into production. A release could be a new software package, an update, a patch, and so forth. The release role also has the responsibility of maintaining accurate inventory management and asset management.

The Risk Management discipline was added to recognize that the management of risk is its own management discipline. ITIL only provides discussion about handling of risk for each IT operations process.

Explicit management review checkpoints are also built into MOF to guarantee that there is involvement by management at each key step in the process. The ITIL books do not include these checkpoints. This is another added value that Microsoft provides with MOF.

THE MICROSOFT OPERATIONS FRAMEWORK PROCESS MODEL

The MOF Process model breaks down a complex environment into an easy-to-manage and easy-to-understand set of functions, thanks to the numerous SMFs that Microsoft added when they created the MOF. SMFs are just a portion of the overall Release Cycle that MOF employs.

Microsoft defines a *release* as any change, or set of changes, that is incorporated into a managed environment. A release includes not only changes in applications or operating system updates, but also changes in operations processes or changes in the physical environment. These releases have a defined life cycle. The life cycle is defined by quadrants, Operations Management Reviews

(OMRs), and SMFs. The four quadrants are essentially categories, defined by the different SMFs that each quadrant contains. SMFs are groups of best practices; each category explains the activities of an operations environment. These quadrants reflect those found in Table 1.2.

The Changing Quadrant

The Changing Quadrant is a group of SMFs that define the proper introduction of approved changes into a well-managed IT environment. This can include changes in applications, hardware, and systems, as well as changes in policies and procedures. The Changing Quadrant maps to the ITIL discipline of Service Support. The three SMFs that reside in the Changing Quadrant are Change Management, Configuration Management, and Release Management.

Change Management The Change Management SMF is intended to place a rigorous process for introducing change into a well-managed IT environment with minimal impact to the operations of that environment. In the most efficient and well-managed enterprises, there are Change Advisory Boards as well as special subcommittees such as the Change Advisory Boards — Emergency committee.

Configuration Management Configuration Management is all about being able to identify, maintain revisions, and track every version of processes, procedures, documentation, hardware, software or any other component within the enterprise. Once this catalog manifest has been achieved, these attributes can become potential Configuration Items (CIs), which then build into an overall model with the environment.

Release Management Release Management is the culmination of Change and Configuration Management to inject or deploy change into the environment. This can be a single change or multiple changes that have been developed, tested, and packaged for a deployment. The goal of Release Management is to record and track changes into an environment with success, accountability, and the least impact possible to the environment.

The Operating Quadrant

The Operating Quadrant is a group of SMFs that are used to monitor, control, manage, and administer service solutions to achieve and maintain service levels. All of the SMFs in the Operating quadrant are items that Microsoft has specifically added to expand ITIL.

System Administration The day-to-day administration of services and systems in an IT infrastructure. This could include user and group account administration; administration of file, print, database, and applications servers; low-level monitoring; and troubleshooting of the systems in the IT infrastructure.

Security Administration The administration of security in an IT infrastructure. This includes monitoring the environment in both a reactive and proactive way, thus ensuring that the environment is safe from attack. This is accomplished in many ways, including identification and authorization control, access control, and auditing.

Service Monitoring and Control The near real-time monitoring and alerting of the health of an IT environment. This SMF ensures that SLAs are in place and that business requirements for IT services are being met.

Job Scheduling The administration and scheduling of jobs and processes so that an efficient sequence is utilized. This could include scheduling batch jobs to maximize system throughput and utilization and to meet SLAs.

Network Administration Administration of the network to ensure that the network operates at an efficient level at all times. This includes the administration of people, processes and procedures, vendors, and service providers, as well as the administration of the network hardware.

Directory Services Administration The administration of resources in Active Directory, such as users, applications, servers, printers, and so forth. The goal of this SMF is not only to make sure that directory access is always available, but also to ensure that information from the directory is available via a simple and centralized process.

Storage Management The administration and control of data, both electronic and physical, for the purposes of restoration and historical archiving. This includes both onsite and offsite storage. Storage Management was put into place to help guarantee the physical security of backups and archives.

The Supporting Quadrant

The Supporting Quadrant is a group of SMFs that identify, assign, diagnose, track, and resolve incidents and problems in a timely manner within SLAs. The Supporting Quadrant maps to the ITIL discipline of Service Support. The three SMFs that reside in the Supporting quadrant are Service Desk, Incident Management, and Problem Management.

Service Desk Almost identical to the Service Desk within ITIL, the Service Desk should be the primary point of contact for an organization to receive customers' problems, concerns, questions, complaints, or requests. This function can also bridge or broker other technical resources that work independently across multiple geographic locations.

Incident Management Incident Management is the process by which, when an issue or occurrence is detected, the correct support resource can address and resolve the incident as quickly as possible. This process allows an organization to better understand the impact an incident has on the overall SLA, as well as mapping recurring issues and potential financial impact.

Problem Management In conjunction with Incident Management, Problem Management leverages the data results from the Incident Management process to trend repeating incidences, prioritize, and analyze root causes. Without this important process, IT can be perceived as a "budgetary black hole" as well as impacting customers' productivity by repeating incidences.

The Optimizing Quadrant

The Optimizing quadrant is a group of SMFs that help maintain business and IT alignment by attempting to decrease IT costs while maintaining or improving service levels. The Optimizing quadrant introduces three new SMFs to help expand the base ITIL disciplines.

Workforce Management This function was added specifically to address staffing issues in the IT infrastructure team. It helps with the process of attracting, developing, and retaining a properly trained and prepared IT staff. It also ensures that the work environment is safe and efficient.

Security Management This function was created to help an IT infrastructure define and communicate the business's security plans and policies, based on the guidelines and regulations that apply to that business.

Infrastructure Engineering Infrastructure Engineering is the conduit and link between the people, process, and technology of an IT Department. These reusable and consistent standards, policies, and procedures in the Infrastructure Engineering SMF could be linked to any other SMF to help coordinate engineering policies and standards.

Service Level Management The process of Service Level Management is where the rubber meets the road. This process defines which services are offered and supported, and at what cost to the business. Most organizations we have spoken and worked with have unwritten expectations or assumptions ("... we expect the application 100% of the time,""... my e-mail is running slow," and so on), but few have well-defined, written SLAs. As organizations start defining and agreeing on service levels, along with seeing the cost of doing business we've seen drastic behavior modifications or acceptance.

Capacity Management The art and process of Capacity Management understands what an organization has and how it's performing, knowing its current and future capabilities, and optimizing for existing and future needs. The art is bringing together business, services, and appropriate, optimized resources, which achieve the agreed SLAs of the customer.

Availability Management As noted previously, it's an expectation within the Service Level Management process for an application to be available 100 percent of the time. So it becomes apparent that Availability Management has become one of the most important aspects with an IT service organization. Availability or the occurrence of an incident has a tremendous impact on customer perception of the IT services being provided.

Financial Management In order for an organization to meet its requirements within the Service Level Management process, there are business demands for fiscal responsibility from a cost and budgetary perspective. In other words, for every request (action) there is a financial impact (reaction). At the end of the day, there needs to be a cost/benefit analysis.

Service Continuity Management Another reason you should work towards achieving a well-defined SLA is preparing for the worst to happen: losing a hard drive, having an incorrect network configuration, having a WAN link trunk cut, or having a network administrator accept another job, for example. A customer or consumer of IT services doesn't really care about the "hows" or "whys" of making things happen; they just want their things to happen.

In order to keep things happening, an organization must adopt a Service Continuity Management process. This ensures keeping the business running or documenting risks which the business is willing to accept when taking an incident. This is a fine balance of resilient systems, failover or recovery options, and risk management.

Operations Management Reviews

Because the Microsoft Operations Framework is depicted as a circle, it is a continually evolving set of processes. Along with the distinct processes, continual customer feedback is always a part of the process in order to further refine them. Along with the four distinct SMF quadrants are the Operations Management Reviews (OMRs), which are process review assessments that include the appropriate stakeholders.

OMRs are either event-based or time-based. The Change Initiation and Release Readiness reviews are event-based and occur at the initiation and final installation of a review into the target environment.

Change Initiation Review The Change Initiation Review is triggered when approval has been requested for a proposed change to the environment. This begins the process of actually

implementing the release. Investments in money, time, equipment, and staff will now begin to work on the process and get it ready for release.

Release Readiness Review The Release Readiness Review determines when a release is confirmed as ready for production. The proposed release is checked to ensure standards, policies, and quality; metrics are in place to support the release.

The Operations Review and Service Level Agreement Review occur at regular intervals to assess the internal operations as well as performance against customer service levels.

Operations Review The Operations Review is a regularly scheduled review to assess and improve IT operations based on business need and SLAs. Operations reviews use information from operations guides, company policies and procedures, and operating-level agreements to measure and evaluate the performance of the operations staff.

Service Level Agreement Review The Service Level Agreement Review is a regularly scheduled review to assess and improve the alignment of business needs with IT service delivery defined in SLAs. During this review, the operations staff and service-level management take current information and measure that against published SLAs to determine whether the service has met its service-level requirements.

Within these four quadrants is a collection of 21 SMFs. Each quadrant consists of a group of SMFs that divide the quadrant into logical procedures and tasks. Each SMF is assigned to a home quadrant, but SMFs are by nature cross-functional and cross-quadrant. If you look back at Table 1.2, you can see how these processes define an SMF, each of which is a series of actions or operations that are designed to achieve a goal. Each process is then broken down into procedures, which allows for coordination between departments. Each procedure has a series of tasks that must be performed to complete the procedure. The *task* is the lowest level of effort on a project.

ITIL VERSION 3 AND MOF VERSION 4

In April 2008, Microsoft released MOF Version 4, which is based on ITIL Version 3. Although there is somewhat of a realignment of service management functions and the like, the basic fundamentals still remain true. MOF v4 consists of four phases that include sixteen SMFs. The four phases and goals are:

Plan Plan and optimize an IT service strategy to support business goals and objectives.

Deliver Ensure IT services are developed effectively, deployed successfully, and ready for operations.

Operate Ensure IT services are operated, maintained, and supported in a way that meets business needs and expectations.

Manage This is the foundation of the IT service life cycle. Provide operating principles and best practices to ensure that the investment in IT delivers expected business value at an acceptable level of risk. This phase focuses on IT governance, risk, compliance, roles and responsibilities, change management, and configuration. Processes in this stage occur during all phases of the life cycle.

Within each phase, service management functions define the people, process, and activities required to align IT services. These functions are shown in Figure 1.1.

FIGURE 1.1 Business/IT Alignment Microsoft Operations Reliability Framework 4.0 Policy Financial Management Operations Envision Service Monitoring and **Project Planning** Control Build **Customer Service** Stabilize Problem Management Deploy Manage Governance, Risk and Compliance Change and Configuration Team

Tying It All Together

Microsoft set out to provide you with tools that help you manage your IT systems. They achieved this by integrating systems management tools and knowledge of the systems to help you with day-to-day operations of the environment, as well as ease your troubleshooting efforts and time and improve planning capabilities. Microsoft took ITIL and MOF, and created a "family" of products — known as the System Center — that helps you in your quest to align with the practices set forth in those documents.

DYNAMIC IT

The System Center family of products helps IT organizations capture and use information to design more manageable systems and automate IT operations. As software becomes more and more complex, thus introducing new components and systems to the infrastructure, the infrastructure will in turn become much more complex. For example, an inventory application moves from being client/server-based, to multi-tier, to a web service-based application. As the application grows and more users start using it, the decision is made to install a hardware load balancer in front of it. Then the data is moved to a Storage Area Network (SAN) to give the IT Department better control over backup and recovery options.

Because of these changes, many different "teams" in the IT Department are involved with this "application." You quickly see how a change to the application can affect more than just the application developers. You now have to coordinate changes with the Web Server Team, the database administrators, the Networking Team, and the Storage Team.

Whether these teams are made up of one person (you), or they are made up of dozens of people, you quickly realize how complex the infrastructure can become, and why there is a need for management of these distributed systems. Dynamic IT is a vision to build software that incorporates ITSM capabilities and MOF best practices with the software (System Center) in order to match IT capabilities and operations with business needs.

Dynamic IT will help IT organizations deliver end-to-end offerings that will:

- ♦ Increase productivity and reduce costs across the entire IT organization
- ♦ Reduce time and effort required to troubleshoot and maintain systems
- ◆ Improve system compliance with business and IT policies
- ◆ Increase responsiveness to changing business demands

SYSTEM CENTER

Before looking at the System Center family of products, let's first look at the different System Center management disciplines that were introduced by Microsoft to help define IT Service Management:

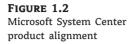
- Operations Management
- Change Management
- Configuration Management
- Release Management
- Asset Management
- Data Protection Management
- Problem Management
- Capacity Management
- Incident Management

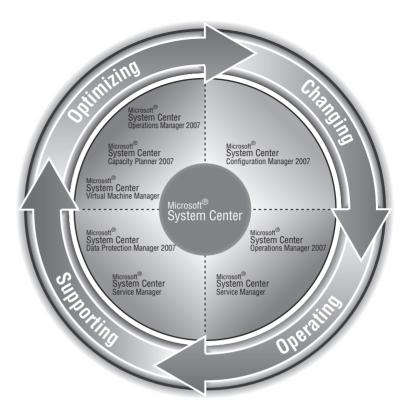
Looking at this list and Microsoft's plan for the System Center family of products, you can quickly see how they have embraced this framework. Through internal products, close work with partners, and acquisitions of software from other companies, Microsoft has addressed each one of these disciplines with products within System Center. As an alignment to the System Center brand, all management products within Microsoft will be rebranded with the System Center logo and family name. As Figure 1.2 illustrates, the Microsoft System Center family is at the heart of management tools.

System Center Operations Manager Formerly Microsoft Operations Manager (MOM). This product provides you with tools to help you proactively monitor your network as well as reduce the complexity associated with managing an IT infrastructure.

System Center Configuration Manager Formerly Systems Management Server (SMS). This product provides a comprehensive solution for the Change Management and Configuration Management disciplines. It touches Release Management and Asset Management as well because it is often used to roll out patches and updates and has a widely used inventory feature.

System Center Data Protection Manager Data Protection Manager (DPM) is a backup and recovery product that gives the end user some recovery options to help take some of the





burden off the IT staff. DPM is a centralized backup solution that captures changed files to disk, providing rapid and reliable recovery. The primary focus is on Microsoft Server and application workloads such as SQL Server, Exchange Server, Virtual Server/Hyper-V, Windows File Server, and SharePoint Portal Server.

System Center Capacity Planner Capacity Planner is a tool to be used in pre-deployment scenarios when planning a new deployment, infrastructure changes, or upgrades. It provides best-practice guidance and hardware-specific knowledge to help planning around Exchange 2003 and 2007, as well as MOM 2005 and Operations Manager.

System Center Service Manager This is another product that touches more than one management discipline. Service Manager will introduce Microsoft's configuration management database (CMDB), which will be populated with data from other System Center products, a workflow engine for automation of IT processes and integration, a common data reporting warehouse, and a self-service portal and knowledge base. Service Manager will address key processes such as Incident Management, Problem Management, Change Management, Asset and Configuration Management, End User Self-Service, and Performance Reporting.

System Center Virtual Machine Manager Virtual Machine Manager (VMM) is a new solution to address managing virtual infrastructures (Microsoft and VMWare), providing a unified management tool for host (physical) and guest (virtual) machines, identification of underutilized hosts, and rapid provisioning of guests.

System Center Mobile Device Manager Mobile Device Manager (MDM) is a new solution that addresses key scenarios inherent to mobile devices. These scenarios include:

- Making a Windows Mobile 6.1 or higher device a fully qualified member of an Active Directory Domain
- ◆ Mobile VPN with dual factor authentication access
- Active Directory Group Policy enablement of over 125 Group Policy attributes specific to mobile devices
- Over the air (OTA) provisioning
- Remote device wipe

System Center Essentials System Center Essentials (SCE) is a new management solution that is targeted at the emerging small to midsize business segment. This solution is designed to manage up to 500 workstations and 30 servers providing unified reporting (i.e. assets, capacity, software deployment, and so on), proactive monitoring, change, and configuration management.

Defining Operations Management

There is often some confusion when it comes to the actual definition of *operations management*. Microsoft's System Center family of products comprises several products that span a wide range of "management" ground. The most confusing overlap of this area is between systems management and operations management. This section looks at the difference between the two.

Systems Management

Systems management is typically defined as software that is used to centrally manage large groups of computer systems. This software contains the tools to control and measure the configuration of both hardware and software in the environment.

Microsoft's solution in this arena is a product called System Center Configuration Manager 2007. Configuration Manager provides remote tools, software update management (otherwise known as patch management), software distribution, hardware and software inventory, software metering, desired configuration management, operating system deployment, and much more. With each capability of Configuration Manager you take advantage of, you can reduce the total administrative effort required to maintain the systems within your environment, thus lowering the total cost of ownership (TCO) of the resources that are being fully managed.

Operations Management

Now that you have an understanding of what falls under the category of systems management, we can focus on operations management. *Operations management* is mainly focused on ensuring that business operations are efficient and effective through processes that are aimed at improving the reliability and availability of IT systems and services. You accomplish this by gathering information from your current systems, having the proper people in place to decipher that data, and having proper procedures in place to carry out any tasks that may arise if there is a current or potential problem in your environment.

The System Center solution that addresses this need is System Center Operations Manager. Operations Manager provides you with the information you need (i.e., performance, security, scalability, knowledge, and so on) to help reduce time and effort in managing your IT infrastructure by automating service tasks and giving you a proactive approach to determining possible problems.

Chapter 2

Planning a Configuration Manager Infrastructure

It has been a common misconception over the years that Microsoft Systems Management Server (SMS), now Configuration Manager 2007, is nothing more than a beefed-up software deployment system. With that assumption, SMS deployments often have not been planned properly and have suffered performance problems. These issues can be blamed on the software itself, the administrator who runs the system, or other factors which will result in a waste of time and resources trying to support an application that was poorly planned in the first place. Properly planning an SMS infrastructure is crucial in utilizing the software to its full potential. This is even more the case with System Center Configuration Manager 2007 (Configuration Manager), with its new and improved features.

In this chapter, you will learn how to do the following:

- Gather deployment intelligence that you will need to plan a Configuration Manager infrastructure for your organization
- Use the deployment intelligence that you have gathered to plan and design a Configuration Manager deployment

Configuration Manager Features

Before you can begin planning to deploy Configuration Manager on your network, you need at least a basic understanding of the features that Configuration Manager provides. For veteran SMS 2003 administrators, these features will not be very different from what you are used to already. However, you will find several new features added to Configuration Manager, several features that were feature packs or add-ins in SMS 2003, and others that have been improved from their previous configuration. Additionally, through the use of the Microsoft Management Console (MMC) 3.0, you'll find home pages for most of the major features, as shown Figure 2.1 as well as throughout the chapter.

The major features include the following:

Inventory Configuration Manager has the ability to inventory the hardware and software of its client computers. Hardware inventory can gather information from your systems such as processor information, the computer manufacturer, and the amount of installed memory. Software inventory can gather lists of file types and their versions installed on your computers, with EXE files being the default. Combine this with extensive information in the Asset Intelligence knowledge base, and you can use Configuration Manager to really get a handle on what kind of hardware and software is being used in your environment. Inventory is the backbone

of Configuration Manager; you can run Configuration Manager without enabling inventory, but you really wouldn't be able to do much, since so many other features, such as software updates, require inventory. Inventory is just about the same as it was in SMS 2003. We will go into more detail about this feature in Chapter 10.

FIGURE 2.1
Microsoft Configuration
Manager 2007 console



Queries Queries allow you to gather information from the Configuration Manager database through the WBEM query language. This allows you to answer questions quickly or make mini-reports that might not be used often enough to be imported into the reporting interface. You can export these reports from the Configuration Manager console into different file formats and then email them for others to use in programs such as Microsoft Excel. Queries are primarily used to make groups of Configuration Manager resources called *collections* that are used by other Configuration Manager features.

Collections Collections can be the answers or results to a question that involves specifying various resources, such as, "Which resources are running Windows XP Professional Service Pack 2 with more than 2 GB of RAM, with more than 1 GB of free disk space, and with a certain BIOS version?" Collections allow you to organize Configuration Manager resources into logical groups, based on a query. A collection can target Configuration Manager tasks to the resources that you specify. You can make collections based on queries, allowing them to be updated dynamically based on a configurable schedule or by directly assigning resources. Collections can consist of computers, users, user groups, or any discovered resources in the Configuration Manager database. Collections, as a fundamental feature, have not changed much since SMS 2003, but they are now the necessary building blocks to use to enable other features such as maintenance windows, collection variables, and others.

Software distribution This feature allows Configuration Manager to distribute just about anything to its client computers. This is probably the most-used feature of all the previous versions of Configuration Manager, and it's probably the most dangerous if not used carefully. It is likely that just about all SMS admins have accidentally deployed a piece of software that they shouldn't have (if you haven't, then keep up the great work!). This isn't a fault of this

feature but something that can happen if you don't test, test, test, and then test again. Anything you plan on deploying to client computers must be carefully managed, and you must pay close attention to the details of what you are doing. It is important to note that Configuration Manager is just the method of distribution; it doesn't have any built-in capability to package software before it is distributed. You will have to use another piece of software to do that yourself. Microsoft has licensed AdminStudio Configuration Manager Edition from Acresso to give administrators a reliable and repeatable tool to assist in creating Windows Installer packages. This, of course, is where the testing comes in. This feature has had numerous improvements since SMS 2003, such as the deployment of not only physical applications but virtual applications as well, but overall it works basically the same as it did before.

Software updates This feature of Configuration Manager has to be one of our favorites. Using this feature, you can manage the daunting task of deploying updates to Microsoft applications and operating systems after the perfect storm that is Patch Tuesday blows through once a month (or whenever updates are released for other applications in your environment). Not only does this apply to Microsoft security patches and updates, but having this flexible and extensible environment has allowed partners (such as HP, Dell, IBM, Citrix, and others) to create custom catalogs to update server and desktop BIOS, firmware, drivers, as well as of the ability to create an internal catalog. This enables customers to create their own line-of-business application update catalogs and update them through the same streamlined process as Microsoft has for patch management.

Deploying updates requires a Windows Server Update Services (WSUS) server, which is a departure from previous versions of Configuration Manager. Configuration Manager leverages WSUS with its own functionality and provides a higher level of granularity than available with WSUS alone. The System Center Updates Publisher upgrades technology developed for SMS 2003 R2 to give administrators the ability to configure custom updates for line-of-business applications as well as configure software for vendors that have partnered with Microsoft to provide update catalogs for their products. These custom updates can be published to WSUS and deployed just like updates for Microsoft products. We will cover software updates in more detail in Chapter 7.

Software metering Software metering, also covered in Chapter 7, allows you to collect information on software usage to assist in managing software purchases and licensing. Using software metering, you can do the following:

- Report on the software that is being used in your environment and on which users are running the software
- Report on the number of concurrent users of a software application
- Report on software license requirements
- Find unnecessary software installs
- Find software that is installed but isn't being used

The new twist to software metering, a departure from SMS 2003, is that the metering rules are autopopulated or created but disabled by default, based on the software inventory. This allows you to rapidly meter applications and gain insights into usage. SMS 2003 had metering, but it was cumbersome to figure out what the appropriate rule setup was. This now is a thing of the past.

Operating system deployment (OSD) This feature was originally released as a feature pack for SMS 2003. It was workable but was a minimalist approach that was sometimes difficult to implement and troubleshoot. Configuration Manager not only has this feature fully integrated into the product, but it becomes a feature-rich, process-driven way to deploy servers and workstations. It leverages other new technology specifically designed by Microsoft to deploy operating systems to computers with multiple options. Originally this feature supported the deployment of desktops only, but it now adds support for deploying servers. With the addition of the task sequencer and driver catalog, you can deploy to bare-metal computers or to ones that already have an operating system installed, as well as deploy software to these computers after they have been configured. This allows you to minimize the number of images for different hardware, and it gives you more granular configuration options. We will discuss this robust feature in more detail in Chapter 8.

Remote control This feature allows computer support staff to remotely troubleshoot problems with users' computers just like they were there sitting in front of the computer in person. This feature has been rewritten from the ground up using Windows Vista "collaboration" technology, meaning it has better performance and reliability than it did in SMS 2003. This feature is still integrated with Remote Assistance and Remote Desktop, and it works pretty much the same as it did in the previous version. One large change to the Remote Tools feature, which has caught some customers off guard, is the removal of the "gold key" (or Ctrl+Alt+Del) feature that allowed a remote admin to unlock a machine from a remote location. This was removed because the underlying operating system security model changed and did not allow this remote functionality because of customer concerns that this was a potential security risk. Thus, the remote procedure call was no longer allowed from an operating system perspective.

Desired configuration management This feature is designed to address configuration drift within the enterprise. Enterprise administrators (workstations and servers) as well as security teams need a tool that enables them to set configuration baselines (based on SOX, HIPPA, GLBA, or other compliancy regulations), deploy machines to an environment meeting these baselines (for example, with local guest account disabled, Windows Integrated Security for SQL Server enabled, and so on), and then detect when these changes occur. Microsoft delivers configuration packs, which jump-start an organization in the compliancy areas mentioned and allow you to set up a baseline of standards for your workstations and servers and audit your environment against that baseline. You can configure your own baselines from scratch, or you can use best practices from Microsoft and their partners in the form of Configuration Manager configuration packs, which can be modified if needed. This feature will be covered in Chapter 12.

Mobile device management This feature allows you to manage mobile devices such as Windows Mobile Pocket PC and smartphones. Inventory, file collection, software distribution, and device configuration are all options with this feature. This was an add-on feature in SMS 2003 and is now fully integrated into Configuration Manager. This feature will be discussed in Chapter 13.

Network access protection This is a new feature in Configuration Manager. It leverages technology built into Windows Vista and Windows Server 2008 that allows you to protect your network from potential threats by not allowing computers to access your network that do not meet certain system health requirements such as having updated antivirus definitions or security patches installed. With this feature also you can enforce certain network protocols. Chapter 14 covers this feature.

Wake on LAN This feature, added to software distribution, was available only by purchasing third-party software in SMS 2003. It allows you to leverage technology built into computer hardware to wake up computers that have been turned off so they can run assigned deployments. Chapter 6 shows how to enable it.

Reporting This feature is great for reviewing the status of the environment, for showing return on investment, and for matching licensing with what is actually installed. It grants visibility into the enterprise with the integration of Asset Intelligence (covered in Chapter 9). This allows you to gain an understanding into licensing (Microsoft and third-party licenses), asset age, Client Access License (CAL) utilization, product families/categories, and much more insightful data. With this feature you can create web-based reports, via Configuration Manager or through SQL Reporting Services that can show all the various data that has been collected by the various other Configuration Manager features, such as software update deployment success or a list of computers of a certain manufacturer. You can also group together commonly viewed reports into "dashboards" for easy viewing with just one click. Numerous reports are already created out of the box, and you can create your own custom reports with a little knowledge of SQL queries. Reporting is discussed in several chapters and is covered fully in Chapter 11.

What's New Since SMS 2003?

Configuration Manager 2007 had an interesting development cycle, unlike any of its predecessors. Because the product group had already nailed a solid, scalable, web-based architecture with SMS 2003, Configuration Manager 2007's development was just a natural progression of features to enrich the product. As the beta builds were delivered to early adopters and then the public, the product group found themselves in a beta cycle that was almost bug free. The number of developers needed to address and support the beta cycle was drastically reduced; thus, they were able to have developers work toward some of the Release 2 (R2) features. R2 was released almost a year after the initial release of the product.

Both SP1 and R2 of System Center Configuration Manager 2007 have introduced significant new features. The following sections summarize what's new in each release.

What's New in Configuration Manager 2007 SP1?

SP1 adds the following features:

- Includes a hotfix rollup for issues with the original Configuration Manager release.
- Includes various design change requests (DCR) to help make Configuration Manager the product that meets customer needs.
- Completes the additional infrastructure groundwork needed to support R2 features such as Asset Intelligence and Application Virtualization.
- ◆ Adds support for Windows Server 2008 as a client and site server.
- ◆ Adds support for Windows Vista SP1 as a client.
- Introduces the out-of-band management feature, which provides powerful management control for computers that have the Intel vPro chip set and Intel Active Management Technology (Intel AMT) firmware versions 3.2 or later.

- ◆ Introduces Asset Intelligence (AI) 1.5, which enables the "software + service" concept into Configuration Manager. Instead of having a static product catalog, the AI catalog now becomes dynamic with updated content on a repeatable basis based on customer synchronization. Additionally, you can configure online licensing data to populate reports in order to provide license reconciliation.
- The evaluation for Configuration Manager 2007 SP1 has been changed to 180 days as opposed to the 120-day limit to evaluate the release-to-manufacturing (RTM) version.
- The Application Compatibility Toolkit (ACT) Connector and the System Center Updates Publisher are no longer included with the Configuration Manager 2007 SP1 installation media.

Within the sections of this chapter as well as the following chapters, we will elaborate on how these features are configured and leveraged within the enterprise.

OUT-OF-BAND MANAGEMENT

A business challenge, which has been a struggle for years, is the ability for software to communicate directly with hardware. Let's say, for example, that you're supporting a worldwide organization and have a centralized help desk. You have a desktop that is thousands of miles away, and the user has contacted you because of an operating system "blue screen." A typical support remediation from years past would be to create a ticket so that a local technician would be able to physically visit the location.

Intel introduced manageability directly into its chip set with the Intel Active Management Technology (AMT) initiative; the direct result was the Intel vPro desktop processor. Intel and Microsoft worked on a strategic management initiative so that software can now communicate directly with hardware. Now, when a user contacts the help desk with that same scenario, a help desk administrator can actively engage and potentially resolve an issue without needing to escalate a ticket to another team.

Configuration Manager leverages four key areas to communicate directly to hardware. These areas may be leveraged holistically within an organization's standard operating procedures for *in-band* and *out-of-band management* to provide a streamlined resolution process. *In-band management* is used when the Configuration Manager Agent is functioning, and *out-of-band management* occurs when software communicates with hardware because no other means may apply. These are the four areas:

- Discovery is an area of out-of-band management that provides an administrator with the ability to achieve discovery on demand. This can be performed on a single machine or groups of machines via a Configuration Manager collection. It also allows you to schedule a discovery so that if the software does not respond, the hardware still can provide the insight into an asset.
- Power control provides the flexibility to allow both scheduled and on-demand power-on capabilities. From a scheduling perspective, this can potentially improve efficiency and data consistency when used in conjunction with other Configuration Manager features such as software distribution, software update management, or operating system deployment. From an on-demand perspective, this enables administrators to wake up, restart, or shut down a remote machine. One area of efficiency that enterprises are increasingly demanding is power management. Thus, the ability to control hardware and software from a single pane of glass becomes an attractive feature.

- Provisioning workstations, either as new assets enter the enterprise or as a means to an end in the remediation process, has become a necessary part of an administrator's role. As the operating system becomes less independent of hardware (that is, the operating system hardware abstraction layer [HAL]), the provisioning process may become more streamlined. With an integrated solution such as AMT and Configuration Manager, a secure, zero-touch setup and provisioning of workstations can be achieved.
- Remote console for out-of-band management enables administrators to perform advanced abilities such as serial over LAN, IDE redirection, BIOS password bypass, and manual power control. This allows an administrator to remotely mount a bootable, troubleshooting image (ISO image); boot into the BIOS to change the boot order; or turn the targeted machine on or off at will.

To that end, when the user contacts the help desk with a nonfunctioning operating system, the help desk administrator can proactively take the appropriate actions. For example, the standard operating procedure might look starkly different from just creating a ticket and dispatching a desktop support technician. It may be that the help desk administrator reboots into the BIOS, leveraging the serial-over-LAN capabilities, and changes the boot order in BIOS so that the network card is the first in the boot order. From there, a diagnostic tool is mounted with IDE redirection, which gives the administrator the insight that the operating system has some corrupt DLLs. Thus, the administrator can then provision a role-based operating system image to this user to re-image the workstation. A process or help desk ticket that might have been very expensive or time-consuming now becomes a streamlined process that results in the user having less downtime and a higher degree of satisfaction with their help desk interaction.

DEPENDENCIES EXTERNAL TO CONFIGURATION MANAGER 2007

To implement a holistic in-band and out-of-band enterprise management system, one that can support users around the world who may or may not be connected to your corporate network, certain dependencies may include different individuals or teams within your organization and may require a deeper conversation about the functionalities you're attempting to provide to the enterprise. The following are these dependencies:

- You must have a Microsoft enterprise certification authority (CA) with certificate templates to deploy and manage the certificates required for out-of-band management.
- ♦ You must have desktop computers with Intel vPro Technology or Intel Centrino Pro Technology, Intel AMT version 3.2 or higher, and the latest Intel HECI driver.
- You must create and configure with the correct security permissions an Active Directory container into which the AMT-based computers will be published. Note that it is not necessary to extend the Active Directory schema for out-of-band management.
- If you will provision new computers for AMT without the Configuration Manager 2007 SP1 client installed, you might need DNS servers that resolve the host name of the provision server to the IP address of the out-of-band service point site system server and a DHCP server with an active scope.
- Windows Remote Management (WinRM) must be installed on each site system server that
 hosts the out-of-band service point role and on any computer that runs a remote Configuration Manager console.
- If the out-of-band service point site system role is installed on Windows Server 2003, this requires Windows Server 2003 Service Pack 2 or higher. If you are running

Windows Server 2003 Service Pack 2, this requires that the QFE 942841 hotfix is also installed.

- Computers that will be managed out-of-band must belong to the site server's Active Directory forest.
- Intervening network devices such as routers and firewalls must allow the traffic associated with out-of-band management activity.
- ◆ Full IPsec environments are not supported.

CONFIGURATION MANAGER 2007 DEPENDENCIES

Once your holistic enterprise management approach is underway, it's time to return focus to the features and configurations that are under your control. Ensure that the following are in place so that when it becomes time to leverage the work from your dependant teams, Configuration Manager is ready to consume those efforts:

- The site must be running Configuration Manager 2007 SP1 and have installed the out-of-band service point.
- If you will provision computers for AMT with the Configuration Manager client, the computers must have the Configuration Manager 2007 SP1 client installed.
- If you will use network discovery to identify computers with management controllers, you must first install the out-of-band service point and configure the AMT provisioning account.

ASSET INTELLIGENCE 1.5

Asset Intelligence (AI), although included within Configuration Manager 2007, now becomes its own node within the Administrator console. This isn't the only new aspect of Asset Intelligence; in addition, Asset Intelligence becomes part of the software + service initiative within Microsoft. The services component of AI is not a fee-based feature but is just another extension of the holistic approach; it includes the following functionality:

- New catalog and license management UI in the Configuration Manager Administrator console
- The ability to customize the local catalog, in other words, create new categories and families
- On-demand or scheduled catalog update synchronization through the Configuration Manager console
- The ability to tap software assets unknown to the catalog and pass them up to the online service for a-sync identification
- The ability to import licensing data from Microsoft and compare it to installed inventory

What's New in Configuration Manager 2007 R2?

Configuration Manager 2007 R2 addresses historical customer feature requests, standardization of Microsoft solutions, and the integration of new technologies within Microsoft. Configuration Manager 2007 R2 truly is the evolution of management technology that was derived from the

architecture of SMS 2003, acquisitions of external technologies, and great leadership and vision. The following list highlights these efforts:

- Application Virtualization management support.
- Operating system deployment enhancements.
- ◆ Client status reporting, which provides a set of tools and Configuration Manager 2007 reports to assess the status of client computers, sometimes referred to as *client health*. Clients that show a change in activity patterns might need administrative intervention.
- SQL Reporting Services reporting, which allows you to report on Configuration Manager activity using SQL Reporting Services.
- ◆ Forefront Client Security integration (reporting).

We'll elaborate on each of these in the following sections.

APPLICATION VIRTUALIZATION MANAGEMENT

Microsoft acquired Application Virtualization (App-V) from an external technology company, Softricity. The initial acquisition delivered the ability to compete in the arena of application virtualization. The acquired solution, although connected to an SMS infrastructure, was really a stand-alone solution. With the newest release of App-V, Configuration Manager 2007 R2 leverages its existing infrastructure and extends the reach to deliver virtual applications:

- Integrates the Microsoft SoftGrid 4.5 feature set into the release of Configuration Manager R2, called Application Virtualization Management (AVM), from an infrastructure perspective.
- AVM allows using Configuration Manager to manage and deploy virtual applications, when possible, to make managing virtual applications for the Configuration Manager admin the same experience as when managing standard or "physical" software.
- AVM has version checking, user-based targeting, and streaming functionality.

OPERATING SYSTEM DEPLOYMENT ENHANCEMENTS

Although Configuration Manager 2007 was good at deploying operating systems, a couple of necessary improvements were needed in order to compete in the marketplace. The following enhancements now round out the offerings of Configuration Manager in the enterprise:

- Support for unknown computers for bare-metal deployments. Prior to R2, if a machine came onto the network via a PXE boot or leveraging boot media, Configuration Manager wouldn't know how to address this machine. With R2, an unknown machine can now be categorized as unprovisioned and receive a task sequence to install an operating system.
- Can now specify credentials on the Run Command Line task sequence.
- Support for multicasting operating system images to PXE environment for well-connected LANs leveraging Windows Server 2008 technologies

CLIENT STATUS REPORTING

An ongoing challenge throughout the years with SMS has been ensuring the client agent health; thus, if a client agent is not functioning, most features are ineffective because a client cannot

perform them. The concept within client status reporting is that there are matrices of client health that are known within Configuration Manager. For example, if the hardware inventory client agent is configured to perform an inventory every seven days and the Configuration Manager client agent has communicated every day for the past three weeks but an inventory has not been received, then any administrator would realize that there is an issue that must be resolved. Client status reporting lends insights into these types of scenarios. It has the following functionality:

- ◆ It was built on the SMS 2003 Client Health Monitoring tool.
- The external service, which is dependent on the Configuration Manager infrastructure, queries site system and Configuration Manager clients for client status on agent activity and overall health.
- The service will report on keys of client activity to help administrators monitor and maintain the health of their Configuration Manager clients.

SQL Reporting Services Integration

SQL Reporting Services (SRS) is an evolution of reporting just as previous technologies have been. The Microsoft management team has standardized on SRS for reporting within the System Center family of products. The SRS integration within Configuration Manager 2007 R2 is the first step in this evolution. The standard reports that shipped with Configuration Manager have been ported over to SRS. Within time, we think the reporting aspects of Configuration Manager will be on par with System Center Operations Manager as far as graphical representations such as graphing and dashboards are concerned. The SRS enhancements include the following:

- SRS adds the new server role Reporting Services Point.
- SRS now offers the ability to convert and/or copy classic SMS reports to Report Definition Language format and publish them to a reporting services point.
- SRS adds a new node under Computer Management called Reporting for accessing the SRS Configuration Manager reports.
- SRS adds the ability to manage, browse, and run SRS Configuration Manager reports from the Configuration Manager console.

FOREFRONT CLIENT SECURITY INTEGRATION

Forefront Client Security was an acquisition to provide enterprise security against viruses, spyware, and the like. Forefront is now integrated into the Configuration Manager 2007 R2 release. This integration comes in the form of a configuration pack to ensure that the proper configuration baselines are met within the Forefront Client Security agent. There are not remediation items such as visibility of client viruses or malware.

Forefront Client Security features and enhancements include the following:

- Forefront Client Security is a separately purchased product from Microsoft that provides unified malware protection for business workstations and servers and also provides critical visibility into threats and vulnerabilities.
- There is lightweight integration between Forefront Client Security and Configuration Manager R2.

- Forefront Client Security provides a Forefront Client Security configuration pack that assesses the states of Forefront Client Security agents on computers that are managed by Configuration Manager R2.
- The Configuration Manager admin can then produce reports that state the overall health of Forefront Client Security clients through the existing DCM reporting infrastructure.

Configuration Manager System Requirements

A big part of the planning process is gathering information on the various system requirements for Configuration Manager clients and servers. It is essential that you factor in these requirements while planning your Configuration Manager deployment so you can plan for hardware upgrades or purchase additional hardware to meet your overall plan for using Configuration Manager in your organization.

Configuration Manager Client Requirements

The hardware requirements for the Configuration Manager client need to be examined just as closely, if not more, as the requirements for a Configuration Manager site server, since the client will be deployed throughout your network. If the clients that you are trying to manage are unable to run because of a lack of system resources, then they will not do you much good and will affect the ability of users to do their day-to-day jobs.

HARDWARE

Microsoft lists the hardware requirements for a Configuration Manager client shown in Table 2.1.

HARDWARE	RECOMMENDED REQUIREMENT	
Processor	300 MHz or faster	
RAM	256 MB or more; 384 MB required if using operating system deployment	
Free drive space	350 MB minimum for new client install or 256 MB minimum to upgrade SMS client, but download cache can get as big as 5 GB by default	

OK, let's be honest here. If you have been in this business for any length of time, you know that Microsoft's hardware requirements are driven mostly by marketing and not by any real-life scenarios. A computer with these specs might run with a Configuration Manager client installed, but it probably won't run *well*. We suggest taking the numbers in Table 2.1 and multiplying them by 4 for more realistic requirements. Doing that, you would get something like the requirements shown in Table 2.2.

Now this might end up being more than what Configuration Manager needs to run properly if you aren't using all of its features, but it is better to have more computer horsepower than you need than force your users to a grinding halt. As you know, you will be the first one they go to if that happens after you deploy the Configuration Manager client.

HARDWARE	MINIMUM REQUIREMENT	
Processor	1.2 GHz or faster	
RAM	1GB or more; 1.5 GB required if using operating system deploy	ment
Free drive space	re 1.5 GB minimum	

TABLE 2.2: Our Recommended Minimum Requirements for Configuration Manager

OPERATING SYSTEM

The following are the 32-bit operating systems, with minimum service pack levels, that are supported as Configuration Manager clients:

- Windows 2000 Professional SP4
- Windows XP Professional SP2
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate
- ♦ Windows 2000 Server SP4
- Windows 2000 Advanced Server SP4
- Windows 2000 Datacenter SP4 (supported but not certified; no hotfix support for Datacenter-specific problems)
- Windows Server 2003 Web SP1
- Windows Server 2003 Standard SP1
- Windows Server 2003 Enterprise SP1
- Windows Server 2003 Datacenter SP1 (supported but not certified; no hotfix support for Datacenter-specific problems)
- Windows Server 2003 Standard R2 SP1
- ♦ Windows Server 2003 Enterprise R2 SP1
- Windows Embedded for Point of Service (WEPOS)
- Windows Fundamentals for Legacy PCs (WinFLP)
- Windows XP Embedded SP2
- Windows XP Tablet PC SP2

Configuration Manager will also run on these operating systems that support 64-bit and Itanium processors (by running 32-bit code):

- Windows XP Professional for 64-bit systems (x64)
- Windows Vista Business (x64)

- ◆ Windows Vista Enterprise (x64)
- ◆ Windows Vista Ultimate (x64)
- ◆ Windows Server 2003 Standard Edition Service Pack 1 (x64, IA64)
- ♦ Windows Server 2003 Enterprise Edition Service Pack 1 (x64, IA64)
- Windows Server 2003 Datacenter SP1 (x64, IA64) (supported but not certified; no hotfix support for Datacenter-specific problems)
- ♦ Windows Server 2003 Standard R2 SP1 (x64, IA64)
- ◆ Windows Server 2003 Enterprise R2 SP1 (x64, IA64)

MOBILE DEVICE

The mobile device client requires almost 1 MB of space to install, plus logging will use another 256 KB. It is supported on the following platforms:

- Windows Mobile for Pocket PC 2003
- Windows Mobile for Pocket PC 2003 Second Edition
- ◆ Windows Mobile for Pocket PC Phone Edition 2003
- ◆ Windows Mobile for Pocket PC Phone Edition 2003 Second Edition
- ♦ Windows Mobile Smartphone 2003 (password management is not supported)
- Windows Mobile for Pocket PC 5.0 (password management for these platforms requires the Messaging and Security feature pack [MSFP])
- Windows Mobile for Pocket PC Phone Edition 5.0 (password management for these platforms requires MSFP)
- Windows Mobile 5.0 Smartphone (password management for these platforms requires MSFP)
- ◆ Windows CE 4.2 (ARM processor only)
- Windows CE 5.0 (ARM and x86 processors)
- Windows Mobile 6 Standard
- Windows Mobile 6 Professional
- Windows Mobile 6 Classic

Configuration Manager Site Server Requirements

In the following sections, we will cover the basic hardware requirements for a Configuration Manager site server. The recommendations that we make are not inclusive and may need to be increased if you plan to host multiple server roles per site server.

HARDWARE

Table 2.3 lists the Microsoft-recommended Configuration Manager site server requirements.

	O	o .	ī
HARDWARE			RECOMMENDED
Processor			2.0 GHz or faster
RAM			1024 MB or more
Free drive space			5 GB (15 GB or more if OSD is used)

TABLE 2.3: Configuration Manager Server Hardware Requirements from Microsoft

Once again, these recommended hardware stats are understated for the task. Except for the free drive space, these stats would probably make a decent secondary site without a problem. Of course, the drive space needed depends on how much software and operating system deployment you are going to be doing.

Webcast on deploying Configuration Manager in July 2007 (www.microsoft.com/events/series/detail/webcastdetails.aspx?seriesid=37&webcastid=2906) gave a much more realistic and granular idea of recommend hardware for a primary site. Table 2.4 outlines these recommendations.

TABLE 2.4: Wally Mead's Configuration Manager Server Hardware Requirements

RESOURCE	MINIMUM REQUIRED	RECOMMENDED FOR LESS THAN 50,000 CLIENTS	RECOMMENDED FOR MORE THAN 50,000 CLIENTS
CPU	Pentium 4	$2 \times 2 \text{ GHz}$	4 $ imes$ 2.8 GHz (dual core)
Memory	512 MB	4 GB	16 GB
Network	10 Mbps	100 Mbps	100 Mbps to 1 Gbps
Free Disk Space	5 GB	2 MB per client	2 MB per client

These recommended stats are pretty reasonable for a primary site with a small (25 or so) number of secondary sites, depending on client load, of course. However, we suggest at least doubling the memory for a central site managing a larger hierarchy with several primary and secondary sites attached to it.

CONFIGURATION MANAGER HARD DISK CONFIGURATION FOR BEST PERFORMANCE

We highly recommend that you configure any primary site system to have *at least* four separate disks for each of the different components of Configuration Manager. Five is ideal, and best practices for SQL Server already recommend having the SQL program and the transaction logs on separate I/O channels. This means separate physical disks, not multiple partitions on the same disk. Doing this will greatly improve the performance of your Configuration Manager installation. Each disk should have the following installed:

- Operating system (at least RAID 1 or better)
- ♦ SMS (at least RAID 1 or better)

- ◆ SQL Server (at least RAID 1; RAID 5 if the SMS database is on the same drive)
- ◆ SQL Server transaction logs (at least RAID 5)
- Software and image packages (at least RAID 5)

Disk I/O was almost always overlooked as a bottleneck for SMS 2003, and it is the same with Configuration Manager. You could have a system with four dual-core processors and 16 GB of RAM, but it won't do much for performance if you have one great big C drive on a RAID array. It would be like trying to force a hurricane through a garden hose.

OPERATING SYSTEM

Configuration Manager site servers must have one of these operating systems:

- ◆ Windows Server 2003 SP1 or SP2 (although a number of updates are required for SP1)
- Windows Server 2003 R2

Windows 2000 Server or Windows 2003 Gold are no longer supported for any site server roles. Other requirements include the following:

- All primary sites now require at least SQL Server 2005 SP2. Other versions of SQL are no longer supported.
- ◆ IIS is required for several Configuration Manager server roles.
- ◆ Microsoft .NET Framework 2.0 is required.
- Microsoft Management Console 3.0 is required.

Gathering Deployment Intelligence

With the information on the operating system and hardware requirements for Configuration Manager, your mission is now to gather the rest of the information required to properly plan your Configuration Manager deployment.

This "deployment intelligence" is extremely important in the success of planning your deployment, and people often overlook this step or don't gather enough information to properly plan for what a company might need to get out of the Configuration Manager system.

Deployment intelligence has three parts, which can be done in any order, or at the same time:

Determine what you need to accomplish with Configuration Manager. To be able to get as much as you need to from Configuration Manager, you really have to know what your company requires from the product to fill the needs of your particular business.

Determine what is on the network now and what has been on it in the past. This is also vital information for your deployment planning. You will need to know things such as what kind of configuration management has been done in your company in the past, how your network is set up, and what kind of clients you are planning on managing.

Get your feet wet, and test Configuration Manager in an isolated lab. Get yourself a test lab and learn about the bells and whistles of Configuration Manager in a safe environment. Get that accidental mass deployment out of your system now, and avoid a "resume generating event" later. You might even find something you didn't know about that can benefit your company in the process.

Determining What You Need to Accomplish

Unfortunately, this means scheduling one of those dreaded meetings with a bunch of people. If your management doesn't initiate a meeting and just tells you, "Here is the software and a server — get Configuration Manager working" (that might sound funny, but it is exactly how one of the authors got started in the business!), then you might have to organize it yourself with all the key people in your IT organization.

Get a good working knowledge of what Configuration Manager can do before the meeting, and be prepared (bring this book with you if you have to) to answer questions. If you don't know the answers right away, take the time to do the research before you answer; it will save you a lot of grief later. If you know of an issue that Configuration Manager can address, don't be afraid to let management know what Configuration Manager can provide your company. You never know who you might impress.

Try to nail down what is expected from Configuration Manager as specifically as possible. Make sure to agree on which expectations are priorities and the time frame that they need to be accomplished. If you don't think a request is possible, then make sure to express that up front. If the requests are something that can't really be measure somewhat accurately, then it might not be something that can be pursued with Configuration Manager. You also have to be able to get some kind of quantifiable result out of what is being requested or it might not be reasonable.

When you are outlining these issues, make sure you know what your budget is and how much time you have for the overall objectives. If the budget and time frame can't be decided on, then you really can't go forward with the Configuration Manager deployment.

Describing the Network

Getting this information might take a while and will involve several departments that will have to provide information to enable you to plan your Configuration Manager properly. The following is the specific information you are going to need:

- Information about past or current systems. What other systems/configuration management software has your company used in the past or is still using now? If you have a current system in place, then get details on that system and how it is configured.
- A diagram of your network's configuration, including LAN and WAN infrastructure, physical configuration, network size, bandwidth available, limits on usage, protocols that are being used, and most important, subnet information. This will be vital to your Configuration Manager deployment.
- Active Directory infrastructure information, such as a diagram of the forests, domains, and Active Directory sites. OU information will be used later for certain Configuration Manager features. The most important thing is to get details on IP subnets for each Active Directory site.
- Security configuration information, such as security settings, Windows security groups, Administrator and Domain Admin accounts, whether the clients have admin rights on their computers, account policies and controls, and the risk threshold for security risks.
- Details on your computing environment, such as information on what kind of servers exist and how they will be handled as clients if at all and workstation information, such as estimated numbers at each location to be managed, what operating system they are using and how they connect into the network, and the geographic footprint of your enterprise.

Personnel information such as the divisions of departments in your company and their members of management and reporting procedures, the structure of the IT department, what the members' duties are, and any standard procedures that are already in place that define any configuration or systems management functions.

Setting Up a Test Lab Environment

Setting up a test lab environment is the most difficult step to achieve. You may face challenges getting management to understand the need to have a good test lab. Even if you do have management's support, getting the actual resources for the lab may be another matter.

A test lab, to be truly effective, must be as close to your actual production environment as possible. This means it must have computers that are representative of what you have in your client environment. If it is at all possible, use the same hardware, software, network configuration, and so on, that you have in your production environment, and make sure that these pieces will be allocated for the specific purpose of testing Configuration Manager and nothing else. Try to include at least one of every piece of hardware platform that you have in the field. Using systems that are the lowest common denominator of what you have in the field will be crucial to see whether your current environment will benefit from a Configuration Manager implementation.

Using the newest beefed-up computers will just give you "inflated" results that will could very well cause issues later if discover that you have hardware in your environment that won't work with Configuration Manager for some reason. Also, make sure that you install all the software that you use in production on the computers in your test lab so you can do application testing if you need to before deploying through software distribution.

This testing might produce results that will show that you need to modify your deployment plans that you have so far to support your company's configuration. Only through this testing do you have the potential to avoid "show-stopping" situations that could crop up before your deployment, which could potentially save your company lots of time and money.

After your Configuration Manager testing is done and you're ready for deployment, hold on to your test lab for dear life, and don't let those resources get reallocated. Having a good test lab at your disposal is a crucial tool for testing things such as Configuration Manager service packs, new feature packs, changes in site configurations, and software deployments, and having a test lab will allow you to make informed choices about further growth of Configuration Manager in your enterprise. This test lab is also a great tool to test disaster recovery scenarios.

Planning the Configuration Manager Deployment

With all the deployment intelligence you have gathered, you are now ready to start planning the actual deployment of Configuration Manager. You will make decisions about the following items:

- ◆ The design of your Configuration Manager site hierarchy
- What Configuration Manager features you will use
- ◆ How you will configure those Configuration Manager features
- How you are going to deploy Configuration Manager
- What methods you will use to discover Configuration Manager clients
- Which methods of deploying Configuration Manager clients you will use
- Which client agents you will enable and how they will be configured

Microsoft includes numerous planning worksheets in its online documentation. These are very useful in helping you gather and organize the data that you need to finish this phase of your planning process. They can be found at http://technet.microsoft.com/en-us/library/bb694186.aspx.

Before you begin planning your Configuration Manager site hierarchy, you need to consider the following issues that will affect the design of your site:

- Active Directory considerations
- Configuration Manager site boundaries
- Methods of resource discovery
- Security of your Configuration Manager site
- Configuration Manager disaster recovery

Active Directory Considerations

When designing your Configuration Manager site, you have to take certain things into account about your company's Active Directory configuration.

WILL YOU USE YOUR AD SITES AS CONFIGURATION MANAGER SITE BOUNDARIES?

If so, document all the AD sites that you want to use, and let your company's AD team verify that these sites aren't temporary and will be stable enough to be boundaries of your Configuration Manager site, if that information was not gathered during your deployment intelligence phase.

WILL YOU EXTEND THE AD SCHEMA FOR CONFIGURATION MANAGER?

Extending the AD schema for use with Configuration Manager allows clients to gather important information on its settings automatically and from a trusted, secure location. We wouldn't consider trying to administer Configuration Manager 2007 without AD schema extensions, because the benefits greatly outweigh any downside. Microsoft recommends extending the AD schema as a best practice for a secure Configuration Manager site.

If you do decide that you want to extend the AD schema for Configuration Manager, then discuss with your AD team just what that involves, and verify that you have the appropriate permissions to do so. If you don't, then work with the AD team to plan on how you want to accomplish extending the schema. (If you are the AD team as well the Configuration Manager admin, have the discussion with yourself. Just don't do it out loud, or people will look at you funny.) We discuss how to extend the AD schema for use with Configuration Manager in Chapter 4.

Features that require Configuration Manager schema extensions include the following:

Automatically publishing Configuration Manager site information to AD A manual method to keep Configuration Manager site changes up-to-date will have to be developed by your organization and maintained by administrator.

Global roaming Without the schema extensions, a roaming client's assigned management point won't be able to find other management points on its level in the Configuration Manager hierarchy or sites higher in the hierarchy. This will prevent a roaming client from downloading software distributions from Configuration Manager sites closer to them on the network. If you have a software deployment that is critical in this situation, it will have to be either pulled across the WAN from their assigned management point or installed manually by support personnel.

Network access protection (NAP) Without schema extensions, Configuration Manager will not be able to publish definitions of what is a healthy client to AD, which in turn would prevent

Configuration Manager from determining whether a client is safe enough to be allowed access to the network. This pretty much makes NAP integration with Configuration Manager useless.

For features that recommend Configuration Manager schema extensions to AD, there are workarounds, although some are more labor intensive than others. The workarounds include the following:

Client installations and Configuration Manager site assignment If AD hasn't been extended, then clients will not be able to find the following automatically:

Client deployment parameters You will have to provide your deployment parameters as command-line switches to ccmsetup.exe (see Chapter 5 for the ccmsetup.exe command-line parameters).

Fallback status points You will have to include the name of the fallback status point with the /FLP switch as a command-line option with ccmsetup.exe.

Management point assignment You will have to install the Server Locator role on a system so that a client will be able to determine its Configuration Manager site assignment. If it can't find a management point in DNS or WINS (publishing management point information in DNS and server locator point information in WINS will help with that), you will have to provide the name of that server locator point with the /SLP switch as a command-line parameter with ccmsetup.exe.

Configuration Manager site mode settings information You will have to provide all native mode information as command-line switches with ccmsetup.exe or use client push to install clients.

Client-to-server port configuration Any changes in the port for client-to-server communication will not be published to AD, so you will either have to reinstall all your clients with the correct port information or use a script to change the port settings on each client before they will be able to talk to its management point again.

Secure key exchange between Configuration Manager sites This security feature is enabled by default, so you will have to disable this feature (which is a security best practice), or you will have to manually exchange parent and child site public keys using Preinst.exe.

If you have extended the AD schema for SMS 2003 but for some reason can't do so for Configuration Manager, then the previous workaround also apply.

ARE YOU REQUIRED TO MANAGE CONFIGURATION MANAGER SITES ACROSS MULTIPLE AD FORESTS?

If you are required to manage Configuration Manager sites across multiple AD forests, then you need to be aware of Configuration Manager's limitations for management across forests and prepare for these considerations:

Communications within one Configuration Manager site Only two options are supported for communication across AD forests within one Configuration Manager site: the System Health Validator point when used with NAP and Internet-based client management, which will support the following site systems being installed in a separate forest from the site server:

- Management point
- Distribution point

- Software update point
- Fallback status point
- Server locator points (not considered a best practice for secure sites)
- PXE service point (not considered a best practice for secure sites)

In either case, even if a two-way trust exists between the forests or if external trusts exist between the two servers' domains, you will be required to set up a Windows user account before the installation will work. Also be aware that there will be some latency in sending status messages between sites, and the site server will take a hit in performance. In the Internet-based client scenario, you will want to add another option for security reasons and enable "Allow only site server initiated data transfers from this site system." This will ensure that all traffic that goes between each server comes from inside your intranet and that no data comes in from an untrusted network. All other site systems must be located in the AD forest. The site server, SMS provider, reporting point, and site database server must also be in the same domain.

Communication between Configuration Manager sites Since data between Configuration Manager sites are signed by default, sites in different AD forests won't be able to get public key information automatically for other sites with which they are communicating. So, you will have to manually exchange keys between the sites using Preinst.exe. Also, you must configure Windows user accounts for site-to-site address, unless both AD forests are configured for the forest functional level of Windows Server 2003 and have a two-way trust.

Support for clients in separate forests Clients that will reside in a different AD forest than their Configuration Manager site will have to be configured as if the AD schema for Configuration Manager has not been extended, as was described earlier in this chapter. If you are using Mixed mode and are using the Automatically Approve Computers in Trusted Domains setting, you will need to configure your management point with an intranet fully qualified domain name (FQDN).

Configuration Manager Site Boundaries

Configuration Manager clients are assigned to Configuration Manager sites by setting up boundaries in the Configuration Manager console on a site-by-site basis, just as they were in SMS 2003. In SMS 2003 you could assign site boundaries based on IP subnets or AD site names. In Configuration Manager, you can also define site boundaries based on an IPv6 prefix or IP ranges.

Your deployment intelligence should go a long way to help you determine which type of boundaries would be the best to define and organize each of the Configuration Manager sites that will be in your hierarchy.

OVERLAPPING BOUNDARIES CAN CAUSE UNKNOWN RESULTS

Configuration Manager site systems do not have to be within a site's boundaries. Also, be careful not to make boundaries overlap and assign clients to only one site boundary. Clients that end up in overlapping boundaries can produce unpredictable results, and you may not be able to manage the client at all.

Methods of Resource Discovery

You will need to decide how you are going to find resources that you want to manage with Configuration Manager. You can use multiple methods at once in any combination, and different methods will discover different types of resources. Discovering a resource doesn't automatically make it a Configuration Manager client.

Configuration Manager Site Security

Configuration Manager has two security modes:

Mixed mode Choose this mode if any of the following apply:

- You do not have a public key infrastructure (PKI) already in place in your environment.
- You have not implemented the certificates that are required by Configuration Manager.
- You have to support SMS 2003 clients.
- You have clients that are running Windows 2000 Professional or Server that can't be upgraded.
- You have site systems that are running IIS that are shared with other systems, and you
 can't use a custom website.
- ◆ You have to use WINS as the method that clients find their management point.
- You don't want your secondary sites to be automatically migrated.

Native mode This mode requires PKI to already be running your environment, but if you are required to support Internet-based clients, then this is your only option. Fundamental security enhancements such as encryption and keys becomes attractive and sometimes a business requirement to lock down corporate data.

Configuration Manager Disaster Recovery

A good disaster recovery plan is essential in ensuring that you minimize the risk and impact of a failure of a site system if it occurs. While you are planning your Configuration Manager system is a great time to discuss a disaster recovery plan so you can set it up at the time of your deployment.

Configuration Manager now uses the Volume Shadow Copy Service (VSS) to create backup snapshots, which allows Configuration Manager downtime to be minimized. Configuration Manager disaster recovery is covered in detail in Chapter 16.

Designing Your Configuration Manager Site

Now that you have gotten the initial site planning out of the way, you can begin the task of actually designing what your Configuration Manager site hierarchy is going to look like. To do that, you need to figure out the number of sites you are going to need to manage your company's resources, the AD sites that are linked to those resources, and a standard convention for naming Configuration Manager sites and site codes that you are going to use. Here are some considerations for planning Configuration Manager sites:

Network bandwidth Historically, an administrator's biggest task was to ensure that SMS was not responsible for consuming all the bandwidth on the network segment (LAN or WAN).

Inevitably, the SMS administrator still was blamed. A well-planned Configuration Manager hierarchy takes into account the remote physical sites and how they are connected to the Configuration Manager infrastructure. Take into account the connectivity aspects, the number of supported resources, and service-level agreements (either in place or anticipated to be in place) in order to drive your design.

The general rule of thumb is to think about transactions in small, medium, and large technical chunks (that is, a small patch is 5 MB, a medium line of business is 200 MB, and a large operating system or application deployment is 750 MB to 3 GB). When assessing a remote site, ask the following questions:

- What's the connectivity between the data center and the remote site?
- What's the supported number of resources?
- What's the business workload (small, medium, or large)?

Once you establish that baseline, you can do some common assessments of potential resources needed or current resources impacted. Obviously, the more bandwidth you have, the happier your users will be when you start sending out Microsoft updates to all of your distribution points. If they aren't happy, then eventually someone will end up in your cubicle wanting answers (take our word on that!).

Small locations Over the past few years, there has been a large shift toward downsizing the remote infrastructure needed in a physical location. These changes can be driven by the need for physical security, lack of environmental support (heating and cooling), reduction in server footprint, or a combination thereof. Some of your remote areas might not be big enough to support a site of their own. In that case, you can assign this site as a boundary of another site that is located nearby.

Client agent settings are "all or nothing" If you have a client agent turned on in your site, then it is on for all the clients on your site, period. If your environment requires that certain clients have different settings, then they will require a separate site.

Clients on your central site It is a common best practice that your central Configuration Manager site does not have any clients assigned to it. The best way to make sure that doesn't happen is to not configure any boundaries for your central site. The purpose of a central site is a single repository where clients can be reported upon from an enterprise perspective.

Supporting multiple languages Another best practice is that you have a separate Configuration Manager site for each language you support.

Consider setting up a holding site If you are upgrading an SMS 2003 hierarchy and you can't upgrade all your SMS 2003 clients right away, you can set up a holding site to manage all of the clients that will continue using SMS 2003 until you are ready to upgrade all of your clients.

Management point client load Microsoft says that a Configuration Manager site can manage about 25,000 clients when using one management point. This increases to 100,000 if you use a management point with network load balancing (NLB). This really depends on the performance of the hardware of your management point and whether the server is running any other Configuration Manager roles.

Number of sites The general rule of thumb for the number of Configuration Manager sites is the KISS principal: Keep It Simple, SMSAdmin! The best practice is keeping the number of your sites to as few as possible.

Naming your Configuration Manager sites Each Configuration Manager site requires a three-character alphanumeric code to identify itself from other Configuration Manager sites. You can use the standard characters A–Z, a–z, 0–9, and the hyphen (-). You can't use Windows reserved names such as PRN, CON, AUX, and NUL. Each one of these site codes must be unique in each Configuration Manager site, so be careful, because Configuration Manager won't check to see whether a certain code has been used before. Be sure of what code you want to use, because you can't change it without uninstalling Configuration Manager and starting over. If you have to reuse a site code, make sure that its information is removed from the System Management container in Active Directory and WINS if necessary. If you don't, there could be a long delay in getting your new site to show up after it is installed.

Planning Configuration Manager Site Systems

To be able to set up your Configuration Manager site to meet its goals (as set by management in your intelligence-gathering phase), you will need to decide what Configuration Manager site systems you are going to need to implement to make the Configuration Manager functions that you need work properly. Configuration Manager site systems have what are called *roles* that define what functionality they provide a Configuration Manager site.

You can assign several roles to one site system, but it will depend on the size of your site and the system's hardware whether it will be able to support those roles. To decrease the load that is on primary or secondary site systems, you can distribute roles to other servers if necessary. Some site system roles are enabled when you install Configuration Manager, and others need to be enabled through the Configuration Manager console.

For details on all the Configuration Manager site system roles, see Chapter 4.

CLIENT INSTALLATION PLANNING

As part of the planning for your Configuration Manager deployment, you will need to determine which method you plan to use to install clients. Deciding this now might even impact your decision about how many Configuration Manager sites you need and where you implement them. All the different methods of client installation will be covered in detail in Chapter 5.

CLIENT AGENT PLANNING

Deciding what Configuration Manager client agents to enable and configure directly ties into your company's goals for what it wants to accomplish with Configuration Manager. Using the information gathered from your deployment intelligence will allow you to decide which client agents will best serve your company's needs and may also affect your site design if more site systems are needed to handle the load of certain functions. At the bare minimum, we suggest using the hardware and software inventory agents, because we consider them the backbone of the entire Configuration Manager system. If you don't enable these agents, a number of other features might not be available for use. All the different client agents will be covered in Chapter 5.

Planning the Configuration Manager Hierarchy

Designing your Configuration Manager hierarchy will require you to identify what servers you want to use as a central site, as primary sites, or as secondary sites as needed. Your deployment intelligence will give you the information you need to decide what locations to place any primary or secondary site so that it will most effectively use the resources allocated to the project. You will have to consider how your sites are linked together and the available network speed between them so you can balance what will be needed to accomplish your goals without impacting day-to-day operations.

To fill in the spots of your Configuration Manager hierarchy, follow these steps:

- Determine whether you need a primary or secondary site at each location in your hierarchy based on the number of current and future clients that are going to be at that site. The geographical configuration of your network sites will probably play a factor as well.
- 2. Examine the logical connections between your sites, and decide on the flow of the site reporting structure.
- 3. Use your deployment intelligence to examine the network connection speeds, and how much network traffic is acceptable, so you can plan site addresses with the proper configuration to keep Configuration Manager traffic under those constraints.
- **4.** Define unique boundaries for each Configuration Manager site to avoid overlap.
- 5. Determine which site system roles you are going to need to accomplish your company's goals for Configuration Manager. You can then figure out where in your hierarchy each site system will be physically located to best meet those goals.

From there you should verify your site design in your test lab to find any potential risks or problems that you might need to fix before production.

Pilot Deployment: Determining How to Deploy Configuration Manager

After you have verified your site design in your test lab, you should plan an initial pilot deployment of Configuration Manager on a small section of your network. Monitor the deployment progress and any potential client problems with your first-level support department.

With the lessons that you learn during your pilot deployment, you'll be able to decide which method of Configuration Manager installation to use for your site deployment. Your goal will be to accomplish the deployment as efficiently as possible while preserving the functionality of any previous methods of system management that you already have in place for as long as needed. The deployment method you use will then help you decide whether you will need additional hardware or personnel resources to do that. There are three methods for installing Configuration Manager:

New deployment You can use this method if you don't have an installation of SMS 2003 in place or you just want to start over from scratch.

In-place upgrade of SMS 2003 You can use this method if one of the following applies:

- You need to maintain the existing SMS hierarchy.
- You want to keep the existing distribution points and SMS site boundaries.
- You want clients to keep their current site assignments.

Side-by-side upgrade of SMS 2003 This method is feasible if you want to install a new implementation of Configuration Manager and migrate current SMS clients over gradually.

- You plan on building a Configuration Manager hierarchy on newer hardware.
- Change your hierarchy to match a new network structure.
- Separate clients that will be using different Configuration Manager features.
- Consolidate your hierarchy into a smaller number of sites.
- Keep current SMS functionality while you roll out your new Configuration Manager site.



A PLAN FOR AN UPGRADE

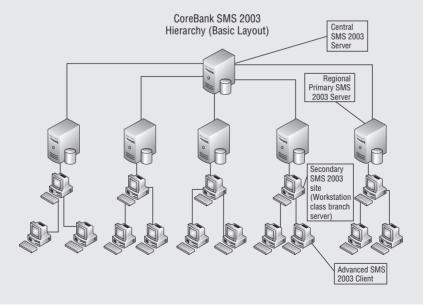
Seeker Inc.'s financial division, CoreBank, is considering upgrading its current SMS 2003 infrastructure to Configuration Manager and needs to make plans before the next budget cycle.

DEPLOYMENT INTELLIGENCE

CoreBank currently has an SMS hierarchy that supports about 5,200 clients, with several regional primary sites that all report to a central site at the company's operations center. Each one those primary sites, in turn, manages secondary sites that are located at each CoreBank branch office, which are primarily being used as distribution points. The central SMS site server has a T1 or faster connection to all the regional primary sites. The connection between each primary and secondary site varies from site to site, with some branch offices having as slow as a 256 Kbps connection.

The central and primary SMS servers were recently upgraded to Windows Server 2003 and are using SQL 2000 SP4. The server's hardware was upgraded as well; the central server got two dual-core Intel Xeon processors running at about 3 GHz and with 8 GB of RAM, and the regional primaries got two dual-core Intel Xeon processors running at about 2 GHz and with 4 GB of RAM. All servers have new SATA or SCSI disk arrays to isolate the separate disk I/O processes, with the operating system, SMS, SQL, SQL logs, and package storage adding up to a little more than 1 TB of disk space per server.

Except for new branch offices that have been recently installed, most of the secondary sites have Windows 2000 Server as their operating system and are workstation-class machines with a minimum 1 GHz processor, 512 MB of RAM, and 80 GB or less total drive space. A basic layout of this hierarchy is shown here.



CoreBank is currently using the following SMS 2003 features:

- Software inventory
- ♦ Hardware inventory
- Software distribution
- Software updates
- Software metering
- Operating system deployment
- Reporting

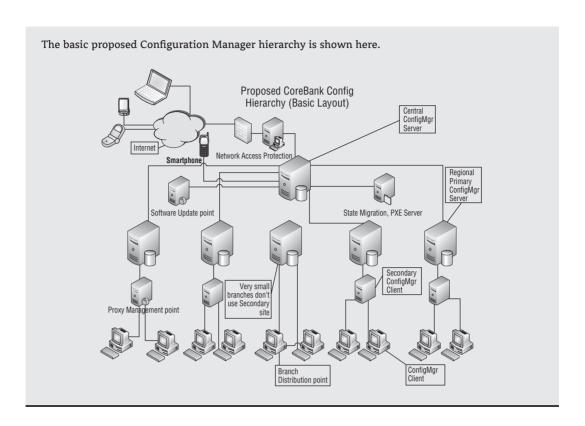
It wants to continue using these features in Configuration Manager, as well as use these new and improved features that are in Configuration Manager:

- ♦ Remote tools
- Desired configuration management
- Mobile device management
- Network access protection
- Wake on LAN

DEPLOYMENT PLANNING

With this information, this book, and information from the Microsoft documentation on Configuration Manager, the SMS administrator for CoreBank knows the following will have to be done before the company can upgrade to Configuration Manager:

- The version of SQL on the central SMS server and on all the primary sites will have to be upgraded to SQL Server 2005 SP2.
- All the secondary sites will have to be upgraded to at least Windows 2003 SP1 (with other updates), with Windows 2003 SP2 being recommended.
- All the secondary sites' hardware will need to be upgraded to accommodate the new and improved Configuration Manager features. They will need machines with at least 2 GHz processors, 1 GB of RAM, and at least enough free drive space to hold all the current packages times a factor of 3 to allow for changes and updates to those packages. The drive space number is a rough estimate, but it should allow for the growing size of the operating system and software update packages.
- Plan for possibly more servers to hold the additional site server roles that are now required for the new and improved features of Configuration Manager, such as the software update point and PXE service point. Those new roles are discussed in detail in Chapter 4.
- Client systems that have hardware or operating systems that do not meet minimum requirements for Configuration Manager will have to be either upgraded or migrated to a child SMS 2003 primary site that will have to be left running to support those clients.
- ♦ As a precaution, possibly double the memory on the central and all the primary servers so they can support the enhanced capabilities of SQL 2005, plus the additional overhead of Configuration Manager.



The Bottom Line

Gather deployment intelligence that you will need to plan a Configuration Manager infrastructure for your organization. Deployment intelligence is extremely important in the success of planning your deployment, and people often overlook this step or don't gather enough information to properly plan for what their company might need to get out of the Configuration Manager system.

Master It What are the three parts of deployment intelligence?

Use the deployment intelligence that you have gathered to plan and design a Configuration Manager deployment. After you have gathered your deployment intelligence, you can use all this information to plan your deployment of Configuration Manager.

Master It If you configure Configuration Manager sites with overlapping boundaries, what could happen to the clients assigned to those sites?

Chapter 3

Interoperability with Systems Management Server 2003

Systems Management Server (SMS) 2003 was a major upgrade to prior versions of the product, and with the upgrade came much pain. There were core infrastructure shifts moving from a "batch processing mode" to web services. Along with the infrastructure changes came client changes as well. The notion of doing delta inventories and sending that XML blob up to a web service, or Management Point, over HTTP port 80 was the "new way." That allowed SMS 2003 to become much more scalable than previous versions. At the end of the day, the product growing pains were worth the wait. We finally had a solid configuration product in which all the features worked very well.

System Center Configuration Manager 2007 R2 builds upon the successes of SMS 2003 and Configuration Manager 2007. The difficulties with SMS 2003 were that we had to deal with enterprises that had not updated to modern technologies. Windows NT domains, Windows 98, and WINS were some of the legacy technologies that needed to be supported. With Configuration Manager, those technologies are not supported and become a thing of the past.

Elsewhere in this book, we focus on a new installation of Configuration Manager 2007 servers and clients. This chapter will focus on migrating existing Systems Management Server 2003 hierarchies and clients. As we drop support for legacy technologies, there are potential pitfalls that you need to address prior to upgrade.

In this chapter, you learn to:

- Describe the three strategies to move to System Center Configuration Manager 2007
- Manage interoperability scenarios
- Plan the site hierarchy
- Upgrade from a prior installation of Systems Management Server 2003

Interoperability with SMS 2003

In Chapter 4, we will cover the prerequisites and installation of System Center Configuration Manager 2007 R2. The first step toward a successful migration/upgrade to Configuration Manager is to decide on your strategy. Some of the criteria to consider include:

- Is the current SMS hardware adequate to sustain a Configuration Manager hierarchy?
- ♦ Does the current data (i.e. inventories, packages, advertisements, histories, and so on) in the SMS database need to be retained?
- Do your current systems (servers and clients) meet the requirements of Configuration Manager 2007?

Once the decision has been made to adopt Configuration Manager 2007 R2 as your organization's change and configuration management tool of choice, there are several schools of thought about how to implement it. If you are a current Systems Management Server 2003 Service Pack 2 shop, there are a few approaches when upgrading from SMS to Configuration Manager. (If you're currently not upgraded to SMS 2003 SP2, you have a little work ahead of you!) These options include:

- ◆ Wipe and load
- ♦ In-place upgrade
- Parallel installation

Each option has its pros and cons. For example, if you do not need to retain the data from the existing SMS database, the wipe and load scenario might be preferred over an in-place upgrade. However, if historical SMS data is business critical, then an in-place upgrade might be the logical choice.

This chapter explores some of the possible interoperability and upgrade scenarios that current SMS customers might encounter during the Configuration Manager 2007 adoption process.

Interoperability Scenarios

We'll cover System Center Configuration Manager 2007 R2 Site Roles in Chapter 5, which outlines all of the site server roles available within the product. These new site server roles grant SMS architects and/or administrators the flexibility to further wrap Microsoft's change and configuration management solution around the business. More roles can potentially introduce more complexity. We are firm believers in the KISS principal: Keep It Simple, SMSAdmin! This boils down to keeping the number of primary and secondary sites at a minimum within your hierarchy. Let's not forget that you can now leverage the Branch Distribution Point in place of building a secondary site server as a Distribution Point whose primary purpose was for software distribution in a small (10 or fewer machines) branch office.

The first priority in designing a Configuration Manager 2007 solution is to fully understand all of the changes as well as the great, new features it brings over SMS 2003. Some of the new architectural features and scenarios include:

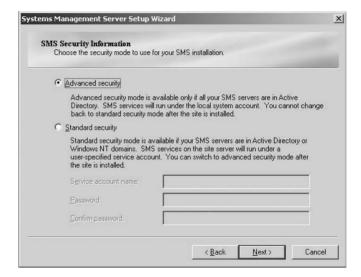
- Branch Distribution Points
- Fallback Status Point
- Maintenance Windows
- Software Update Point
- Network Access Protection
- Multicast-enabled Distribution Point
- Application Virtualization-enabled Distribution Point
- Integration with Intel's AMT out-of-band solution
- Client Status Reporting
- SQL Reporting Services Reporting
- Forefront Client Security Integration
- Asset Intelligence Integration

In Chapter 5, we'll cover the installation and configuration of all of the site roles. Without the knowledge of these redesigned or new features, the architecture can be severely impacted. Out-of-band management was introduced in Chapter 2, and other new features will be covered throughout the book.

SITE SECURITY

In Systems Management Server 2003, an administrator chose from two Site Security modes: Standard or Advanced, as noted in Figure 3.1. The preferred security mode was Advanced security mode, because it leveraged Active Directory, Local System accounts, and machine accounts as security principals.

FIGURE 3.1 SMS 2003 Site properties security



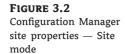
Additionally, there were two SMS 2003 clients: Legacy and Advanced. These were required in order to provide most of the legacy support, both for infrastructure and the client operating system.

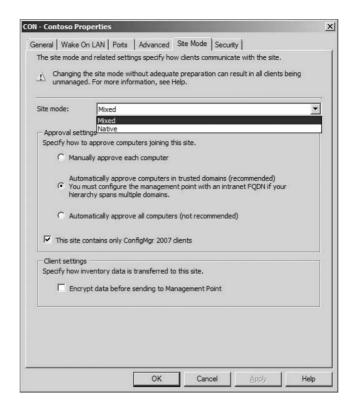
Configuration Manager 2007 R2 has one security mode, from a client perspective, which is comparable to the SMS 2003 Advanced Security model. As in most of the features in Configuration Manager 2007, the best-of-breed approach was taken. This model provides the most secure infrastructure as well.

Configuration Manager 2007 has two site modes to choose from: Mixed and Native. As shown in Figure 3.2, this mode can be selected and changed to or from Native mode at any time. This is a different approach to site security than you see in SMS 2003. The major difference between the Mixed and Native security mode is that the Native site mode leverages certificates as the means for authentication. This difference will be apparent and a prerequisite for Internet Client Based Management in a later chapter.

SITE BOUNDARIES AND SUPPORTING ROLES

SMS 2003 added many levels of complexity when it came to site boundaries, roaming boundaries, local/remote boundaries and regional/global roaming concepts. These settings and concepts allowed clients to use local resources as much as possible and provide fail over to their assigned site as needed. The following sections review the SMS 2003 foundations.





Global and Regional Roaming Concepts

Global and Regional roaming types are merely concepts that are only leveraged by the Advanced Client. There are no specific settings in the SMS Administrator console to enable or disable these roaming types. Global roaming is used by clients that roam to sites that are outside their assigned site hierarchy and have published boundary and MP information to Active Directory. Regional roaming is used when clients roam to sites that are below their assigned site in the hierarchy. In Regional roaming, the client queries its assigned sites default MP to find the site code of the site that the client is currently roaming to.

Global Roaming Once the Active Directory has been extended and sites have published their information to it, clients can use this information to obtain site assignment and access packages.

Advanced Clients use this information for site assignment and to query local MPs for package information. When an Advanced Client roams outside its assigned site boundaries and requires access to a package, it queries AD to find the resident site's default MP and submits a content location request to this default MP. Any site in an Active Directory forest that publishes site information to AD can be queried by any Advanced Client within that forest. This allows clients to install software from local sources regardless of their current location in the infrastructure.

Regional Roaming When a client roams to a site that is below its own assigned site, it will request information from its assigned site's default MP about the site it has roamed to. The assigned site contains information about all of its child sites and will provide the site code of

the site that the client has roamed to. Regional Roaming clients will then query AD or WINS to find the resident MPs to request content as needed. When clients travel to other sites that are not child sites of the client's assigned site, they will only be able to send inventory (across the network) and run packages that had been previously downloaded or fall back to using the assigned site s DP.

Local Roaming Boundaries

Local or Remote Roaming Boundaries define the location of a DP to the specified boundary. Advanced Clients that fall within a Local roaming boundary will determine that DPs for that boundary are local. Any Roaming Boundaries that have DPs on a fast, reliable connection to the client should have the boundaries defined as Local.

Remote Roaming Boundaries

Remote roaming boundaries are used when you want to include clients in the Roaming Site Boundaries but there is no local DP. Clients within the remote roaming boundaries will only run advertisements that are specified to run from a remote DP. Remote boundaries are primarily used in small office locations with limited bandwidth and no local DP access.

Fallback Situation

When an Advanced Client is outside of all known boundaries, it will only install advertisements that have already been downloaded or that the client is set to install from a remote boundary.

Protected Distribution Points

When specifying a server to act as a Distribution Point site system, it can also be enabled as a Protected Distribution Point. This allows you to specify site boundaries or IP subnets that the client must be within to utilize the DP for package source files. You can select only those boundaries that are already configured for the site. This gives the administrator more control over which clients use specific distribution points. This setting is recommended for dial-up RAS solutions to make sure all RAS clients use a specific DP, which ideally would be the closet DP.

As an example, let's say we have a single site with 5000 clients dispersed over five physical, geographic locations. We could have five distribution points enabled for the site. We could allow the clients to randomly select an available DP, but this might allow clients to overload a single DP. The protected DP setting allows us to balance the load by restricting client access by selecting available site boundaries or IP Subnets for specific Distribution Point servers. Thus, if a client requests software files, the restriction of a client traversing the WAN to access those files may be negated.

Configuration Manager 2007 Boundaries

One of the first configuration changes that might catch a veteran SMS administrator's eye is the location of the option for setting Site Boundaries. Historically, this setting was awkwardly placed in the Properties of the Site Server, requiring a right-click. This has finally been addressed and moved into the Site Settings area within the Configuration Manager Administrator Console.

In stark contrast to the way Boundaries functioned in SMS 2003, Configuration Manager 2007 has only one type of boundary that is similar in comparison to an SMS 2003 Roaming Boundary. This boundary is then defined by its connection type, either Fast (LAN) or Slow Or Unreliable, as shown in Figure 3.3.

FIGURE 3.3 Configuration Manager New Site Boundary Dialog

Description:						
Site Code:	CEN-Cor	itoso He	adquart	ers Site		•
<u>I</u> ype:	IP subne	t				•
<u>N</u> etwork:	Г	- 01	10	60	_	
Subnet <u>m</u> ask:	Г	-		24	_	
Su <u>b</u> net ID:	Г		- 10		-0	
Network Connection Clients in this boun Clients or un Fast (LAN)	dary comn	nunicate	with the	e site by	using a netwo	rk that is:

Note that upgraded SMS 2003 Primary Site Boundaries cannot be modified within Configuration Manager 2007. This upgraded boundary will be read only until it is deleted and/or recreated as a Configuration Manager 2007 Boundary.

On the other hand, when you're addressing and potentially upgrading the Secondary Sites from SMS 2003 to Configuration Manager 2007, Secondary Site Boundaries can be managed with Configuration Manager 2007.

COLLECTIONS

The foundations of the collections feature have not changed significantly from SMS 2003 to Configuration Manager 2007. A few default collections have been dropped (All Windows 98 Systems, All Windows NT Systems, and so on); a few have been added (All Desktops and Servers, All Windows Mobile Smartphone 5.0 Devices, and so on), and the remaining core collections have not changed (i.e., All Windows 2000 Professional Systems, All Windows XP Systems, and so on).

During the upgrade process, any default collection that has undergone any modifications will retain its customization(s). Any default collection that has been deleted will be recreated.

CLIENTS

Because Configuration Manager 2007 R2 was built upon the successful architectures of SMS 2003 and Configuration Manager 2007, there is only a single client within Configuration Manager 2007 R2. All the attempted legacy support within SMS 2003 has been removed. Thus, the SMS 2003 Advanced Client with all the appropriate service packs and hotfixes has become the Configuration Manager 2007 R2 client.

Prerequisites for Configuration Manager 2007 Clients

Along with dropping a few default collections, collections are mirrored for the supported, associated client operating systems. The following Microsoft Legacy Operating Systems are supported on a 32-bit platform only:

- Windows XP Service Pack 2
- ♦ Windows 2000 Professional Service Pack 4
- ◆ Windows Embedded for Point of Service (WEPOS)
- ◆ Windows Fundamentals for Legacy PCs (WinFLP)
- ♦ Windows XP Embedded SP2
- ◆ Windows XP Tablet PC SP2
- ♦ Windows 2000 Server Service Pack 4
- ♦ Windows Advanced Server Service Pack 4
- Windows 2000 Datacenter Service Pack 4

The one exception to the rule is that Windows XP Professional for 64-bit systems is legacy but only 64 bit.

The following current operating systems are supported on 32-bit and 64-bit platforms:

- Windows Vista Business Edition
- Windows Vista Enterprise Edition
- Windows Vista Ultimate Edition
- Windows Vista Business Edition Service Pack 1
- Windows Vista Enterprise Edition Service Pack 1
- ◆ Windows Vista Ultimate Edition Service Pack 1

The following current operating systems are supported on 32 bit, 64 bit, and IA64 bit:

- Windows Server 2003 Standard Edition Service Pack 1
- Windows Server 2003 Enterprise Edition Service Pack 1
- ◆ Windows Server 2003 Datacenter Edition Service Pack 1
- Windows Server 2003 R2 Standard Edition
- Windows Server 2003 R2 Enterprise Edition
- Windows Server 2008

The exception to this rule is that Windows Server 2003 Web Edition, Service Pack 1 is 32 bit only.

Hardware Inventory

Over the years, SMS administrators have become very savvy with the SMS MOF (Managed Object Format) and modifications thereof. There are customizations for inventorying DIMM slots, local accounts, locally attached printers, and the list goes on and on.

When upgrading existing clients, these customizations do not migrate into Configuration Manager 2007 because of changes in the hardware inventorying. To avoid losing the customized data sets, disable the Hardware Inventory Client Agent within the SMS 2003 site before upgrading to Configuration Manager 2007. Once the upgrade has completed, modify the Configuration Manager MOF and then enable the Hardware Inventory Client Agent.

Because of the hardware inventory changes within Configuration Manager 2007, a full hardware inventory will be requested from each client once each client has upgraded itself.

There are two separate MOF files within Configuration Manager 2007: configuration.mof and sms_def.mof. The first, configuration.mof, is the definition file; it describes which data classes are targeted for inventory. This file must define and register the WMI providers used to perform and query the computer details during a hardware inventory. The file is a part of the client policy body, which Configuration Manager 2007 clients download and compile automatically.

The sms_def.mof file defines the reporting classes and attributes to be inventoried. It is based on the configuration.mof's existing data classes. When the file is manipulated or extended, as mentioned previously, it must be recompiled on the Configuration Manager 2007 client systems.

SMS 2003 SITE SERVERS AND SETTINGS

If you are currently running SMS 2003, it is important to note which features are currently installed and configured. It is also important to note which features in Configuration Manager 2007 R2 are going to be leveraged so a seamless transition can occur between the two products.

Hierarchy Management As in any upgrade to SMS, the work must be performed from the Central or top-most Primary Site within the SMS 2003 hierarchy. If the Central Site has clients reporting to it, there may be a data storm of hardware inventories which may backlog the server until they can be processed. This is why a thorough understanding of the features and interoperability issues which may arise are critical to your success from moving off of SMS 2003 and onto Configuration Manager 2007.

If there are multiple SMS 2003 Primary sites within the hierarchy, be aware that the Configuration Manager 2007 console cannot manage an SMS 2003 site. It may be necessary to install a remote instance during the migration period.

Existing Data Data which might have been placed within the SMS 2003 folder structure (i.e., patch packages and source files) over the course of time will be deleted once the upgrade has completed. It is possible to install Configuration Manager 2007 into another directory, which will retain all of the pertinent information.

Active Directory Schema If the Active Directory schema was not modified by the current installation of SMS 2003, now would be an opportune time to modify it so Configuration Manager 2007 may leverage it.

SMS 2003 FEATURE PACKS

SMS 2003 introduced new features, called Feature Packs, which were outside of the upgrade to SMS 2003. These features are the SMS 2003 Operating System Deployment and SMS 2003 Device Management Feature Packs. Their features have been fully incorporated into Configuration Manager features, so part of the prerequisite process is to remove the feature packs before moving to Configuration Manager 2007.

Planning the Upgrade from SMS 2003 to Configuration Manager 2007

This section describes the steps required to verify Systems Management Server 2003 site upgrade readiness, upgrade from SMS 2003 to System Center Configuration Manager 2007, and extend the Active Directory schema to include Systems Management Server objects.

During this section we will introduce the Deployment Readiness Wizard, examine the different upgrade scenarios and their impact on your infrastructure, and discuss Active Directory extensions for Configuration Manager that allow SMS site information to be published in the Active Directory.

Identifying Configuration Change Requirements

Some of the changes in Configuration Manager 2007 include additional server roles, server role modifications, and platform support. Before you upgrade an SMS 2003 site to Configuration Manager 2007, you can use the Installation Prerequisite Checker to identify potential problems and determine corrective actions. The Installation Prerequisite Checker can be run against a Primary Site, Secondary Site, or Administrator Console workstation (see Figure 3.4).

FIGURE 3.4 Configuration Manager Installation Prerequisite Checker Options-Upgrade



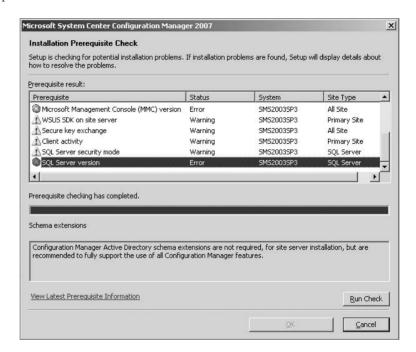
INSTALLATION PREREQUISITE CHECKER FEATURES

At the beginning of the Setup process, the Installation Prerequisite Checker should be run against your sites before you perform the actual site upgrade. This utility uses a series of rules to determine whether the site can be upgraded successfully. Test results are displayed within the Checker as well as logged in the ConfigMgrPrereq.log on the root of the system drive on the machine which it ran. This log contains the Errors and Warnings, which were recorded during the check. Additionally, a registry setting contains the number of Errors, Warnings and Failures, Report path, and Time Stamp of when the Installation Prerequisite Checker last ran. This can be found at:

If the Configuration Manager 2007 upgrade process reads values greater than 0 for the error entry, the upgrade process will terminate. To allow the upgrade process to continue, all reported errors must be resolved and the Installation Prerequisite Checker must be run again to reset the values.

As shown in Figure 3.5, a link within the Installation Prerequisite Checker called "View Latest Prerequisite Information" connects to a complete listing of all the prerequisite check rules and descriptions that are performed.

FIGURE 3.5
Configuration Manager
Installation Prerequisite
Checker results



USING THE INSTALLATION PREREQUISITE CHECKER

To run the Installation Prerequisite Checker:

- Locate and run setup.exe (located in the SMSSetup\Bin\<PLATFORM> directory on your source media).
- 2. On the Welcome splash screen, click Run The Prerequisite Checker.
- **3.** The option for Upgrade will be selected. Check All Secondary Sites to run the Installation Prerequisite Checker against all Secondary Sites within the hierarchy. Select OK.
- **4.** Once the Installation Prerequisite Checker has completed running, in the Prerequisite Result area, double-click the Warning or Error, which will present the details of the particular issue.
- If any Errors have been detected, they must be addressed before you can advance with the upgrade.
- 6. Select either OK or Cancel.

Running the Installation Prerequisite Checker from the Command Line

You can also run the Installation Prerequisite Checker from the command prompt. Locate and run Setup (setup.exe) with one of the prerequisite switches from Table 3.1. All command-line options are described in Table 3.1.

TABLE 3.1: Installation Prerequisite Checker Command-Line Options

COMMAND-LINE SYNTAX	When used
Setup.exe/prereq	Verification of prerequisites for upgrading.
<pre>Setup.exe/prereq/pri/sql <sql name="" server=""></sql></pre>	Verification of prerequisites when installing a new Primary Site Server. Additionally, this option will verify that the Primary Site Server computer and SQL Server meet prerequisites.
Setup.exe/prereq/pri/sql <sql server name>/mp <mp name="" server=""></mp></sql 	Verification of prerequisites when installing a new Primary Site. Additionally, this option will verify that the Primary Site Server computer, SQL Server, and Management Point computer meet prerequisites.
Setup.exe/prereq/sec	Verification of prerequisites when installing a Secondary Site server.
Setup.exe/prereq/ui	Verification of prerequisites when installing a new Configuration Manager console.

Setup /TestDBUpgrade

Prior to upgrading your SMS 2003 site to Configuration Manager 2007, we recommend that you validate that the SMS database will successfully upgrade. The setup program for Configuration Manager 2007 includes the /TESTDBUPGRADE switch. This switch is used to run a test upgrade against a replica of the SMS database. The upgrade testing process cannot be run on your SMS site server and will not proceed if it determines that the SMS Provider is installed on the machine.

To test the upgrade of the SMS 2003 database, perform the following steps:

- **1.** Back up your SMS database using one of these methods:
 - ◆ Use the backup of the site database created by a recent SMS backup task.
 - ◆ Stop all SMS services on the SMS site server. Use SQL Server Enterprise Manager to back up the SMS database.
- **2.** On another computer running the same version and service pack of SQL Server, restore the database that you backed up using the following method (noting that you do *not* need to install SMS on the computer on which you will restore the database):
 - **a.** Create a new database with the same name as the database to be restored.
 - **b.** Set the default data/log file sizes to 1MB when creating this database.

- c. Restore the database using SQL Server Enterprise Manager. If the drive letters differ between original location and location being restored to, you may need to modify the destination drive and file properties during the restore.
- Once the database has been restored on the test server, run the following from a command prompt:

Setup.exe /testdbupgrade <database name>

Running setup /testdbupgrade will fail if the SMS site database has been restored from a backup of an SMS 2003 site database on which the original SQL Server had database replication enabled. When SQL Server replication is enabled for an SMS 2003 site database, the computer running SQL makes modifications to the SQL tables included in publication. For this reason, when the database is restored to another database on a different SQL server, the /testdbupgrade switch will fail. To work around this problem, you should disable publishing of the SMS site database prior to commencing the backup.

If the database upgrade test is successful, the database portion of the process on your actual site will also be successful. Any problems detected by the test upgrade must be corrected prior to commencement of the actual upgrade. The results of the /testdbupgrade process can be determined by reviewing SMSSetup.log stored on the root of the system drive on the SQL test server.

Planning Your Upgrade Strategy

As noted previously, the Installation Prerequisite Checker displays Errors and Warnings for all issues that may prevent successful upgrade. Once all Errors and Warnings identified by the Installation Prerequisite Checker have been resolved, you are ready to plan and implement site upgrades.

As noted in Chapter 1, any well planned upgrade/migration leverages a well thought out project plan. These should be based on a solid foundation or methodology such as Microsoft's Operational Framework.

The initial steps in any project are a typical gap analysis. They fall into three basic categories which you must ask yourself:

- Where are you?
- Where do you want to be?
- How do I get there?

A thorough project plan should include some or all of the following phases as well as work tasks for each phase:

Phase 1: Define and Capture Phase

- Create project plan.
- ◆ Document current environment.
- ◆ Conduct initial risk review.
- ◆ Create business test cases.
- Finalize business proposal.

Phase 2: Build Phase

- Conduct planning workshop.
- Install a Proof of Concept lab.
- Conduct server and workstation testing.
- Procure hardware.

Phase 3: Test Phase (Pilot)

- Draft communication plan.
 - Executive/Management
 - ◆ Project team
 - ◆ Site (User)
- Build and deploy hardware and software.
- ◆ Change control
- ◆ Pilot

Phase 4: Production Deployment Phase

- Change control
- ◆ Site deployment

Phase 5: Post Review Phase

- Lessons learned
- Project reflection (party)

One fundamental part of a project plan that is commonly overlooked is the Communication Plan. This is used generally in two different ways: first, to inform users of what is changing on their desktops, but more important, as a communication vehicle to show the value that you bring to the business! Use this project to highlight the capabilities of Configuration Manager 2007 as well as the business value and insights of reporting, software updates, and software distribution. Don't be afraid to highlight the hard work and value that a project of this magnitude brings to the business.

Types of Upgrades

Three main upgrade strategies are available to deploy Configuration Manager 2007 to an existing infrastructure:

In-Place Upgrade This is the simplest method to upgrade SMS 2003 servers and clients. An in-place will retain all SMS 2003 hierarchy, settings, packages, advertisements, and data for use in Configuration Manager 2007.

Side-by-Side Migration A side-by-side migration creates a new Configuration Manager 2007 infrastructure that runs side by side with the SMS 2003 infrastructure. This migration allows clients to be managed 100 percent of the time while the migration is being conducted.

Wipe and Load The wipe and load approach is useful if the end goal is to start over with change and configuration management. Thus, there will be zero data saved or migrated.

Upgrade Guidelines To ensure a successful upgrade, consider the following guidelines before you begin:

Parent sites must be either the same version as or one version later than their child sites. For example, a Configuration Manager 2007 site can function as parent site to either a Configuration Manager 2007 or an SMS 2003 child site. However, an SMS 2003 site cannot function as parent site to a Configuration Manager 2007 site.

Systems Management Server 2003 Service Pack 2 or later must be applied to all sites prior to starting the upgrade. All sites within the hierarchy must be at SMS 2003 SP2 or later if they will co-exist at any time.

Upgrades must be performed in top down fashion. If you are upgrading a multi-tier hierarchy, you must start at the central site and work your way down through the site hierarchy.

Using the In-Place Upgrade Strategy

The In-Place Upgrade strategy upgrades the targeted SMS site to a Configuration Manager 2007 site in a single operation.

This strategy requires minimal planning and only a small window of time. It is recommended for environments where:

- ◆ The hierarchy includes only a few sites (a relatively flat hierarchy).
- Infrastructure plans have not been finalized.
- Existing hardware is adequate to run Configuration Manager 2007

IMPLEMENTING IN-PLACE UPGRADE

It is important to note the new security, client, and hardware requirements needed for Configuration Manager 2007. Ensure that all clients and servers meet minimum requirements such as those related to client operating systems and service packs.

After the SMS 2003 servers are upgraded, SMS 2003 clients will install upgraded client components automatically during their next Client Configuration Installation Manager (CCIM) maintenance cycle for upgrade to the Configuration Manager 2007 Client. The entire SMS 2003 hierarchy and all clients should complete upgrades to SMS 2003 within 25 hours. If client computers can be left on and connected to the network, you can schedule Overnight Upgrade to begin on a Friday evening and allow ample time for clients to install upgraded client components over the weekend.

RESOLVING UNSUPPORTED CLIENT PLATFORMS

Before beginning any upgrade process, you must identify clients running on unsupported platforms such as Windows 98 or lower and Windows NT 4.0 and determine whether or not to use a holding site for these clients.

If the site to be upgraded includes clients running on unsupported platforms and these clients cannot be upgraded prior to site upgrade, you must first establish a holding site to continue managing these clients.

MODIFYING DEFAULT SITE ASSIGNMENTS

When an SMS 2003 client is upgraded to a Configuration Manager 2007 Client, the first site that the client was originally assigned to will be used as its assigned site. If you want to override this assignment, you can specify the desired site code during client installation.

PERFORMING AN IN-PLACE UPGRADE

After all the planning, staging, communicating and piloting has been completed, the time has come to roll into one of the final phases of the project plan. The Production Deployment Phase should be a non-event if all of the work prior to this has been completed successfully. The following steps outline an in-place upgrade:

- 1. Insert the System Center Configuration Manager 2007 DVD or run splash.hta from the root of the electronic media.
- 2. Select Configuration Manager 2007 from the Install section of the menu that is presented.
- The Welcome to the Microsoft System Center Configuration Manager 2007 Setup Wizard appears. Select Next.
- **4.** On the Installation Prerequisite Check Options, the Upgrade An Existing Configuration Manager or SMS 2003 Installation radio button is selected. Select Next.
- Read and scroll down through the Microsoft Software License Terms, select I Accept These License Terms, and click Next.
- **6.** The Customer Experience Improvement Program Configuration dialog box appears with the No, I Do Not Want To Participate Right Now radio button selected. Choose either No or Yes depending on your corporate policy. Select Next.
- 7. Enter the 25 character Product Key, which has been assigned. Select Next.
- **8.** On the Settings Summary page, the list that is presented reviews the Setup Components that were selected. Select Next.
- 9. Review any fatal errors, errors, or warnings that are presented (although part of your homework was to run the Installation Prerequisite Checker and address all errors) or review the ConfigMgrPrereq.log on the root of the system drive to see which errors need to be addressed.
- **10.** Review the Installation Status section to ensure the installation is proceeding properly.

Using the Side-by-Side Migration Strategy

In a Side-by-Side migration, an existing SMS 2003 implementation can function while client systems are moved from SMS 2003 to Configuration Manager 2007. This enables you to do the following:

- Use new hardware or continue using the same hardware
- Modify your existing hierarchy

- Retain historical client data
- ◆ Redesign the SMS hierarchy
- Retain custom objects within SMS 2003

This upgrade strategy is most useful when existing hardware will be reconfigured or new hardware will be installed in conjunction with site hierarchy modifications. A great deal more planning is required for a side-by-side upgrade than for the other two strategies to ensure that all clients continue to be managed throughout the process. Before selecting this strategy, make sure that both you and your organization are fully prepared and have given careful and deliberate consideration to all factors, including the following:

- SMS 2003 and Configuration Manager 2007 should not have any overlapping Site Boundaries.
- Updating Site Systems within Active Directory, DNS and WINS.

In a Side-by-Side Upgrade, a new site is brought online in parallel with the existing infrastructure. Clients are then steadily migrated to the new site by adding boundaries on the Configuration Manager 2007 site and removing them from the old SMS 2003 site.

If you use this strategy, clients may be assigned to both SMS 2003 and Configuration Manager 2007 sites. However, clients that successfully upgrade to Configuration Manager 2007 client components and find themselves assigned to an SMS 2003 site will no longer report to the SMS 2003 site regardless of assignment. After upgrade, clients will not remain as members of their original SMS 2003 sites if they find themselves assigned to a Configuration Manager 2007 site.

In addition to adding and dropping Site Boundaries, there are a few variations to the sideby-side migration you can explore. For example, if one of the business goals is to retain hardware inventory histories, an SMS 2003 site can be attached as a child site to the parent Configuration Manager 2007 site. Because inventories, hardware, and software are forwarded up the hierarchy, this will accomplish the business goal of retaining these histories. Another business driver might be to retain custom collections or software distribution objects. To achieve this objective, install a new Configuration Manager Primary Site Server with new hardware to support the end goal of it being the Central Primary Site or the hierarchy. With the SMS 2003 Primary Site that has the custom collections and/or software distribution objects that are to be retained, upgrade this site to Configuration Manager 2007. Attach the projected Central Site Server with new hardware to the upgraded SMS 2003 Primary Site Server. Collections and Software objects flow down the hierarchy, yet there is no need to worry about other data (i.e., hardware inventory, software inventory, and so on) cluttering the new Configuration Manager database. Once these objects have been populated, break the Parent/Child relationship and migrate the clients just as you would in a typical side-by side-migration. This will allow collections and software distribution objects to migrate to the new Configuration Manager database.

Because the clients are currently managed by SMS 2003, there is nothing stopping you from conducting a software distribution of the Configuration Manager 2007 client to targeted machines and forcing them to be assigned to a Configuration Manager 2007 site. Additionally, you can advertise the ccmclean.exe Microsoft Resource Kit utility for SMS 2003 to uninstall the SMS 2003 client from targeted workstations or servers.

Real World Scenario

MIGRATIONS

In some cases, you use a combination of upgrade strategies and product features. For example, if there's a business need to retain current inventories yet move to newer hardware, a case can be made to perform one of two blends:

- Backup and restore on new hardware.
- Create a Parent/Child relationship between the current SMS 2003 Site and new Configuration Manager 2007 Site.

The first presented blend would restore your current SMS 2003 implementation to new hardware and then perform an In-Place Upgrade to accomplish getting onto Configuration Manager 2007 R2. The "downside" to restoring an existing SMS 2003 Site is that all the data will be restored — including inventories, packages, programs, collections, and so on. This can be undesirable depending on the circumstances.

In the second blend presented, a new Configuration Manager 2007 R2 Site could be built on new hardware. Next, the current SMS 2003 implementation could be configured as a Child Site and the new Configuration Manager 2007 R2 Site would be the Central/Primary Site. This scenario enables you to maintain the inventories for historical purposes without bringing over any potentially misconfigured data such as collections or packages. There are utilities and scripts that can be used to export these items from SMS 2003 and import then into Configuration Manager 2007 R2.

Once the Configuration Manager 2007 R2 Site's Parent/Child Relationship is set up, Site Boundaries can be moved or dropped from the SMS 2003 Site and defined on the Configuration Manager 2007 R2 Site. Thus, clients can be migrated over to the Configuration Manager 2007 R2 implementation seamlessly.

Using the Wipe and Load Strategy

The Wipe and Load Strategy is the most basic and straightforward of any of the approaches. Generally speaking, this strategy is intended for environments where SMS 2003 is a single server solution and zero percent of the existing data (i.e., collections, inventories, packages, and so on) needs to be retained, and the clients don't need to be managed 100 percent of the time during the migration. Although this approach may seem like "the path of least resistance," there are a few pitfalls that you need to stay aware of:

Client Manageability If the wipe and load approach is taken, the quickest way to accomplish it is to perform a software distribution to run the ccmclean.exe Microsoft Resource Kit utility for SMS 2003 on all SMS 2003 clients. This poses a potential problem that the clients will remain unmanaged until the server (current or new future hardware) is rebuilt and Configuration Manager 2007 is installed and configured properly. Depending on the environment, this might be a non-issue. A risk assessment would need to be performed to see if a mission-critical

application updates or zero day exploit patches needed to be deployed, and the potential impact to your enterprise. If the risk can be minimized or negated, then a wipe and load might be possible.

Implementation timeframe To rebuild a server and install/configure all the components that are required to support a Configuration Manager 2007 installation is no small task. Not to mention that if you have a strict change control process, this might hinder your forward momentum significantly. All these factors equate to dollars — money spent rebuilding, installing, configuring and testing a server that was already up and running in production.

The bottom line is, just because the wipe and load "appears" to be the path of least resistance, don't be tempted. Think and weigh your options before coming to a decision that you might regret at a later time or day.

Upgrading the Administrator Console

As in the Configuration Manager 2007 Site Server itself, you must consider the upgrade of all the SMS 2003 Administrator consoles to Configuration Manager 2007 Administrator Consoles. This potentially is an area for automation or an unattended installation routine.

Any of the setup functions (Primary Site, Secondary Site, or Administrator Console) can be scripted with an initialization file to answer key questions of a setup routine. In this scenario, we want to automate the Administrator console setup for Configuration Manager 2007.

The following steps will enable you to perform an unattended installation of the Configuration Manager 2007 Administrator Console:

- Ensure that Administrator workstations meet the minimum requirements for the Configuration Manager 2007 Administrator Console. In order to run the Installation Prerequisite Checker to verify the workstation, setup.exe /PREREQ /UI can be performed from the command line.
- 2. Create the setup initialization file in Notepad. This file must contain the following text only:
 - * [Identification]
 - * Action=InstallAdminUI
 - * [Options]
 - * SMSInstallDir=<Installation directory>
 - * ParentSiteServer=<Primary Site the console will connect to>

Of course, the text within the greater than and less than symbols must be removed (including the <> symbols) and replaced with your site-specific information.

3. Advertise the setup of Configuration Manager 2007 with the following command line, substituting the <> text with the name and location of the file from above:

```
"\SMSSETUP\BIN\I386\setup.exe /script <location and name of initialization file> /nouserinput",
```

The following steps enable you to perform a GUI installation of the Configuration Manager 2007 Administrator Console:

Ensure that Administrator workstations meet the minimum requirements for the Configuration Manager 2007 Administrator Console. The Installation Prerequisite Checker will run as part of the GUI installation.

- 2. Insert the System Center Configuration Manager 2007 DVD or run the splash.hta from the root of the electronic media.
- 3. Select Configuration Manager 2007 from the Install section of the menu that is presented.
- **4.** The Welcome to the Microsoft System Center Configuration Manager 2007 Setup Wizard appears. Select Next.
- On the Installation Prerequisite Check Options, select the Configuration Manager Console radio button. Select Next.
- Read and scroll down through the Microsoft Software License Terms, select I Accept These License Terms, and click Next.
- 7. The Customer Experience Improvement Program Configuration dialog box appears with the No, I Do Not Want To Participate Right Now radio button selected. Choose either No or Yes depending on your corporate policy. Select Next.
- **8.** On the Settings Summary page, the list that is presented reviews the Setup Components that were selected. Select Next.
- 9. Review any fatal errors, errors, or warnings that are presented (although part of your homework from above was to run the Installation Prerequisite Checker and address all errors) or review the ConfigMgrPrereq.log on the root of the system drive to see which errors need to be addressed.
- **10.** Review the Installation Status section to ensure the installation is proceeding properly.

Post Upgrade or Installation Considerations

Once you have performed the selected installation, it is imperative to maintain its health moving forward. The obvious choice for performance and availability monitoring is Microsoft System Center Operations Manager 2007.

First review the Site Status from within the System Status node in the Configuration Manager 2007 console. Review all of the Site System Roles to ensure that they are identified properly as well as the Component Status. If there are any critical or red components, right-click the targeted component and select Show Messages > Errors. This produces all of the error Status Messages, which highlight the problems within the Site. You'll find more detailed troubleshooting coverage in Chapter 21.

Another area of concentration should be within the Site Settings. With the new functionality and roles within Configuration Manager, there are a plethora of settings to setup and configure. A more detailed and in-depth view of Site Settings is covered in Chapter 4.

The Bottom Line

Describe the three strategies to move to System Center Configuration Manager 2007 There are three basic paths to get from SMS 2003 to Configuration Manager 2007. As covered in this chapter, it's not always a choice of just one; sometimes you must use a combination of tools within your arsenal. Don't forget that it might not always be a perfectly straight line from Point A to Point C.

Master It A current implementation of SMS 2003 has been running within the enterprise for the past several years. Unfortunately, the Central Primary Site Server does not meet

the minimum hardware requirements necessary to run Configuration Manager 2007 R2. Your manager wants to retain all of the work done in SMS 2003 for historical and reporting purposes. Which of the three strategies could be leveraged to migrate to Configuration Manager?

Manage Interoperability Scenarios Within this first step of "Where are you?" an administrator must identify what system requirements are needed in order to install and run Configuration Manager 2007 R2. Although the system requirements for installing Configuration Manager R2 may not seem like they represent the hardware you would want to run your Configuration Manager system on, you should be aware of the hardware and software requirements so that you know which systems in your environment can support it.

Once the minimum requirements are identified, they must be mapped to the current SMS 2003 installation to ensure the appropriate hardware, software, and licenses are in place. This should include documenting the current SMS 2003 infrastructure with a tool such as Microsoft Visio. Microsoft has created a connector for Visio to connect into an SMS 2003 hierarchy and automatically create an infrastructure diagram.

Master It An environment that contains 5,000 machines and is geographically dispersed over 10 states has Microsoft SMS 2003 Service Pack 1 running on Microsoft SQL 2005. The hierarchy is a single Primary Site with nine Secondary Sites at each of the remote locations. What are any potential interoperability scenarios which might exist?

Plan the Site Hierarchy Configuration Manager 2007 R2 brings a wealth of new features and functions to enable organizations to have a well-managed enterprise. When addressing the question of "Where do you want to be," these features support business scenarios or business pains such as managing mobile workforces outside of the physical corporate networks, addressing governmental or organizational compliancy, and standardization of operating system configurations. A successful administrator or a successful project will typically address a scenario or set of scenarios and use them as success criteria which Configuration Manager 2007 R2 will address.

Master It An environment that contains 5,000 machines and is geographically dispersed over 10 states has Microsoft SMS 2003 Service Pack 3 running on Microsoft SQL 2005 Service Pack 1. The hierarchy is a single Primary Site with nine Secondary Sites at each of the remote locations. Currently there is a mix of client operating systems from Microsoft Windows 98 to Microsoft Windows Vista. What might be the plan to get the enterprise managed by Microsoft System Center Configuration Manager 2007 R2?

Upgrade from a prior installation of Systems Management Server 2003 Force yourself to produce a project plan in order to address the lasting questions of "How do I get there?" Forcing yourself to write out a project plan makes you think critically of the end to end tasks that need to be completed to move from SMS 2003 to Configuration Manager 2007 R2 successfully. Share this plan with peers, your manager, or the Change Review Committee. A project plan is always better when many sets of eyes have looked it over.

The next step of the process is to execute your well-defined project of migrating from SMS 2003 to System Center Configuration Manager 2007 R2. If you've followed the guidelines thus far, the execution should be the easiest part. Use one of the supported methods to upgrade.

Last, and most important, is to celebrate your successes. As in the previous step, once you've identified what went well from the entire project, celebrate the success of your project and enjoy all the rich features of System Center Configuration Manager 2007 R2!

Master It An environment that contains 5,000 machines and is geographically dispersed over 10 states has Microsoft SMS 2003 Service Pack 1 running on Microsoft SQL 2005. The hierarchy is a single Primary Site with nine Secondary Sites at each of the remote locations. Each remote office has approximately 5 to 25 clients, which are the remote sales force. Which new Configuration Manager 2007 R2 roles might be taken into consideration upon a successful upgrade?

Chapter 4

Installation and Site Role Configuration

Microsoft Systems Management Server (SMS) 2003 brought an entirely new architecture to the table. It went from a robust batch processor in SMS 2 to a highly scalable web services architecture. Although SMS 2003 was innovative, it still had to address and support legacy systems.

Configuration Manager 2007 no longer has to deal with a lot of the legacy baggage that was required in SMS 2003. All legacy support (Windows 9x, prior versions of Windows 2000 Service Pack 4, prior versions of Windows XP Service Pack 2, and prior versions of Windows Server 2003 Service Pack 1) has been dropped, except that you can manually add Configuration Manager site information to WINS. Just to be clear, Configuration Manager does not require WINS; for organizations that are not going to leverage the Active Directory schema modifications or DNS publishing, this is the last type of name resolution still supported. To that end, some of the legacy site server roles have been eliminated.

Without having to bridge and support legacy systems, Configuration Manager 2007 can completely focus on addressing core business scenarios, including some that involve pain as well as innovation. Some of those scenarios include the branch office and Internet-facing clients. To address and support these scenarios, Configuration Manager 2007 introduces some new site roles in addition to some of the SMS 2003 site roles.

In this chapter, you will learn how to do the following:

- ◆ Identify the different types of Configuration Manager 2007 sites
- Define Configuration Manager 2007 site relationships
- Configure Configuration Manager 2007 site relationships
- ◆ Enable and configure the essential Configuration Manager 2007 site system roles

Configuration Manager 2007 Site Types and Site Relationships

Since Microsoft SMS 1.0, we've had the notion of a site type being either a *primary site server* or a *secondary site server*. If you boil everything down to the simplest definition of the differences between a primary and a secondary site server, you could say that a primary site server has SQL and a secondary does not. As we progress through the chapter, you'll see some subtle differences between site types, but this is the most rudimentary difference.

At least one Configuration Manager 2007 primary site server must be installed in a Configuration Manager network, because there must be a relational database (Microsoft SQL 2005 Service Pack 2) to store all the site information and client information. A single primary site can manage up to roughly 100,000 clients.

A second site may be introduced for various reasons; any of the following may be true of the organization:

- ◆ Its enterprise is larger than 100,000 clients.
- ♦ It needs the second site to support separate administrative responsibilities.
- ◆ Some remote locations have more than 25 clients.
- ◆ Some remote locations have slow WAN connections.

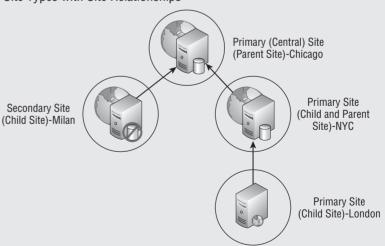
When a second Configuration Manager site is required, whether that site type is primary or secondary, the enterprise is considered a *hierarchy*. A hierarchy is set up in such a way that an organization can manage and report on all its assets. Within a hierarchical relationship, a given site can be a *parent*, *child*, or both, as illustrated in Figure 4.1.

HIERARCHY AND RELATIONSHIP TIPS

The topmost primary site within a hierarchy is known as a *central site*. This is the enterprise repository, which holds all the asset information (hardware inventory, software inventory, patch inventory, and so on) and status.

FIGURE 4.1 Site types with site relationships

Site Hierarchy
Site Types with Site Relationships



A primary site can be a parent, child, or both within a hierarchy. This flexibility is possible because the site has SQL installed, so it can store information locally as well as forward information up to

its parent. Each primary site can have its own version of a *managed object file* (MOF), the definition file that enables the attributes in hardware inventory to be taken. We cover managed object files in greater detail in Chapter 10.

A secondary site can be a child site only. That's because it does not have a repository to store information prior to forwarding to its parent. The Configuration Manager 2007 client uses a secondary site only as a resource. Generally speaking, think of a secondary site as a proxy point.

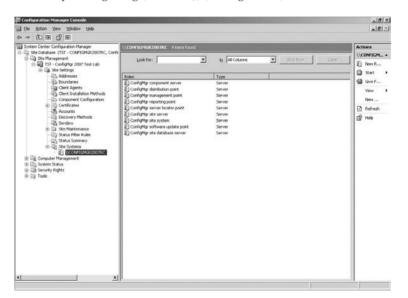
As part of planning your Configuration Manager 2007 architecture, you must decide how you will support the managed clients in your environment. In Chapter 2, we covered some design decisions that you must make prior to implementing Configuration Manager 2007 in a production environment.

Site System Roles

The ability to designate various site system roles to different servers within Configuration Manager 2007 allows it to become distributed and highly scalable.

As stated before, with a distributed architecture comes complexity. A distributed architecture may be necessary to scale to the client count or to provide a higher level of performance by distributing a single or multiple roles to multiple servers within a hierarchy. These roles can be viewed in two separate places, the Site Systems node in the Configuration Manager console (see Figure 4.2) or within the Hierarchy Manager log (hman.log) (see Figure 4.3).

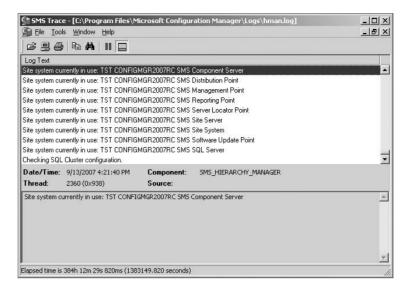
FIGURE 4.2
The Site Systems node within the Configuration
Manager 2007 console



Site Server

Each Configuration Manager 2007 site will have exactly one server running the site server role. This is the server designated to manage the clients within its configured boundaries.

FIGURE 4.3
Reviewing the Hierarchy
Manager log for site
system roles



SOFTWARE REQUIREMENTS

Configuration Manager 2007 site servers have the following requirements:

- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- ♦ Microsoft Management Console (MMC) 3.0 must be installed.
- NET Framework 2.0 must be installed.

IMPLEMENTING A CONFIGURATION MANAGER 2007 PRIMARY SITE SERVER

A Configuration Manager 2007 hierarchy starts with the installation of the first primary site server. When a second physical location with resources to be managed is added, this may introduce another Configuration Manager site, which can be another primary or a secondary site. If a secondary site type is chosen, a default relationship is established; it becomes a child site of the primary site. By contrast, establishing a parent-child relationship between two primary sites is a manual process.



SYSTEM CENTER CONFIGURATION MANAGER 2007 HIERARCHY AND DESIGN SCENARIO

Once you have digested all the site types, site relationships, and site roles completely, you then can apply the theoretical knowledge to a practical application. Most System Center Configuration Manager 2007 implementations will contain more than one site. To scale the solution out while protecting the WAN, it is necessary to establish a hierarchy.

In the following implementation sections of this chapter, you will learn how to create a primary/central site on a dedicated Windows Server 2003 member server running SQL 2005 Service

Pack 2 or higher with a site code of CEN. Leveraging a second physical or virtual server, you'll create additional sites and/or roles on either the secondary server or the primary site server. The second server will need to have all the prerequisites installed and configured in order to function in all of the Configuration Manager roles aside from a primary site.

The criteria to review, when defining network architecture, are the physical sites, WAN configuration, number of users or managed resources, and types of activities planned to support these users. The activities may be as simple as hardware and software inventories or as complex as deploying operating systems and large software applications on a daily basis to these resources.

In this scenario, the enterprise has two physical offices. The primary office contains 600 employees, and the remote office has 50 employees. They are connected via a T1 line, which is 40 percent saturated. You will configure a System Center Configuration Manager 2007 hierarchy to support their change-management needs. Those needs include all the rich features Configuration Manager 2007 provides, including hardware/software inventory, software deployment (patch and application), operating system deployment, and software metering.

The recommended solution is to implement a Configuration Manager 2007 primary site server at the central office while rolling out a secondary site server to support the remote office's needs. It could be argued that a branch distribution point could be used instead of a secondary site server. However, there is a WAN link, which is 40 percent saturated, as well as 50 clients within the remote office. A branch distribution point running on a client operating system (Windows XP or higher) has an inbound connection limit of 10 concurrent connections. Couple this with a highly used WAN link, and the solution lends itself to a distributed architecture. Other issues such as server infrastructure at the remote office, technical support personnel, and political factors may weigh in the decision. The decision to implement a secondary site was driven by the ability to schedule and throttle the WAN traffic from the primary to secondary site. Thus, creating a primary and a secondary site server is the potential solution.

IMPLEMENTING A SITE SERVER: PREREQUISITES

The first stage in implementing the scenario described in the sidebar is to install all the prerequisites:

- **1.** Log onto the physical or virtual server.
- 2. Click the Start button, and choose Control Panel.
- Open the Add Or Remove Programs applet, and select Add/Remove Windows Components.
- **4.** Highlight Application Server, and click Details.
- **5.** Highlight Internet Information Services (IIS), and click Details again.
- **6.** Select the Background Intelligent Transfer Service (BITS) Server Extensions box.
- 7. Scroll down, and highlight World Wide Web Service; then click Details.
- 8. Select the Active Server Pages, WebDAV Publishing, and World Wide Web Service boxes.
- 9. Click OK three times to return to the Windows Components Wizard, and click Next.
- 10. Insert the path to the Windows Server 2003 media if prompted.

- 11. Select the Finish button in the Completing the Windows Components Wizard.
- 12. Close the Add Or Remove Programs applet.

IMPLEMENTING A PRIMARY SITE SERVER

With the secondary server's prerequisites taken care of, let's get to what you are really interested in: installing your first site server. Just like most of the Microsoft wizard-based installations, setting up Configuration Manager is not difficult. As a matter of fact, the installation wizard is pretty easy to work with. Choosing the right options at the right times is what becomes difficult. To compound this problem, there are three different types of setups: simple installation, custom installation, and unattended installation.

Simple Installation

The *simple* installation will perform a very quick and painless installation, but you should take note of what it does. Every role is installed on a single computer using a simple setup. It also configures the site for automatic client-push installation, which means that any system that is discovered will have the client installed. You have no control over the installation — only that, once discovered, the client will be automatically installed during the next discovery cycle. The following list details everything that the simple setup does:

- Installs a primary site server
- Installs the Configuration Manager 2007 site database on a local SQL Server default instance
- Installs and enables the management point and distribution point site server roles on the site server
- Enables the client-push installation method
- Enables common Configuration Manager 2007 client agents; by default, the following client agents are enabled:
 - Software inventory
 - Hardware inventory
 - Advertised programs
 - Software update
 - Software metering
 - Desired configuration management
 - Remote tools
 - All discovery methods, except network discovery

Please note that site boundaries are not created during the simple setup. To perform the simple setup, you need to access the installation files, either on your local machine or shared at a network location.

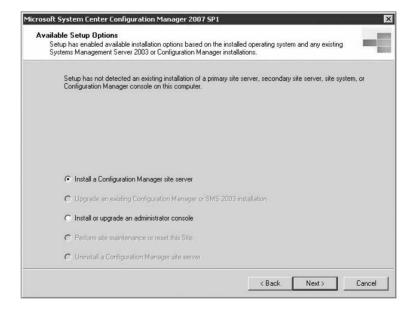
 Double-click the Autorun program, and you will be presented with the splash screen shown in Figure 4.4. Of the options here, click the Configuration Manager 2007 SP1 link, under the Install section, to initiate the setup. Once the Welcome page appears, take note of the instructions, and then click Next.

FIGURE 4.4
The Autorun splash page



2. The Available Setup Options page will appear, as shown in Figure 4.5, giving you the option to perform tasks within the site. Your site configuration will determine which options appear on this page. For this exercise, select the Install A Configuration Manager Site Server option, and then click Next.

FIGURE 4.5The Available Setup Options page



3. The Microsoft Software License Terms page shown in Figure 4.6 appears, giving you the opportunity to review the licensing agreement that you are placing yourself under if you agree to install Configuration Manager. Notice that you also have the ability to print the license agreement by clicking the Print License Terms button. Select the I Accept These License Terms check box, and then click Next.

FIGURE 4.6
The end user license agreement

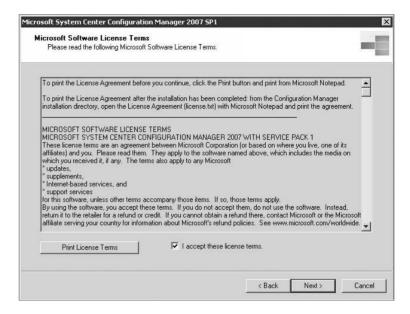
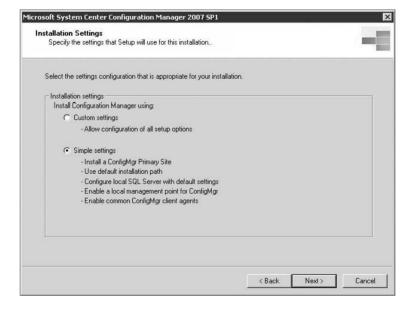
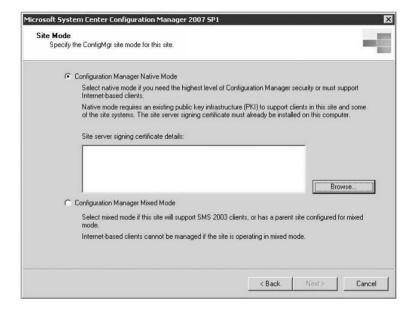


FIGURE 4.7The Installation Settings page



- **4.** The Installation Settings page that appears gives you the opportunity to choose between the Custom Settings and Simple Settings options. Notice that if you choose to go with the Simple Settings option, you don't have very much control over the installation criteria. As Figure 4.7 shows, the simple setup installs a primary site using the default file path, configures the SQL Server with the default options, enables automatic client push, and enables all the client agents. For this exercise, select this option, and click Next.
- 5. The Site Mode page that appears allows you to choose between Native and Mixed modes, as shown in Figure 4.8. If you have decided that Native mode is how you want to configure your site, you need to have a server signing certificate available already. Click Browse to locate the certificate to use, and then click Next. Otherwise, you can choose to use Mixed mode. Note that you will have to use Mixed mode if you have SMS 2003 site systems residing within the site.

FIGURE 4.8
The Site Mode page

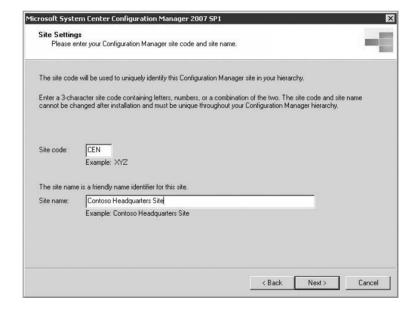


- **6.** Enter the product key that you have been given in the five text boxes on the Product Key page, shown in Figure 4.9. Click Next once you have entered the key.
- 7. The last of the configuration pages is the Site Settings page, shown in Figure 4.10. Here you configure the three-character site code that will be used by all of the site systems and agents; you also have the option to specify a longer descriptive name in the Site Name text field. A three-digit code is usually not enough for us humans to be able to identify something.
- **8.** After you click Next on the Site Settings page, you will see the Summary page. Not much detail is shown here, since you chose the Simple Setup option. Verify that this is what you were planning on performing; then click Next to install Configuration Manager on the system.

FIGURE 4.9
The Product Key page

rosoft System Ce	nter Configuration Manager 2007 SP1		
Product Key Specify the pro	duct key for this Configuration Manager installation.		
Enter your 25 ch	aracter product key:		
Key:	man man man	05	
	< Ba	ack Next>	Cancel

FIGURE 4.10
The Site Settings page

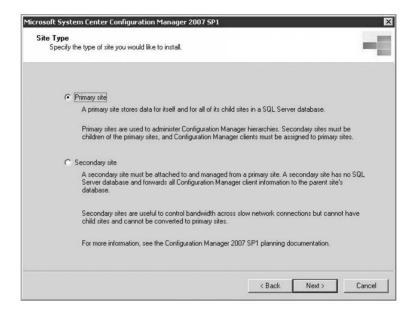


Custom Installation

Needless to say, most production environments will not use the simple installation. It may come in handy for a small network, but most of the time anything outside a test environment will use a *custom* installation. There are far more options to consider when selecting the custom setup option, but you have much more control over how your Configuration Manager installation is configured.

- 1. The installation procedure starts the same way as the simple installation that you performed in the previous section, until the point where you select the installation type (the Installation Settings page, shown earlier in Figure 4.7). If you select Custom Settings there, the subsequent pages allow you more flexibility and control over the installation.
- **2.** The first page that appears after you click Next on the Installation Settings page is the Site Type page, shown in Figure 4.11. It is here that you can choose whether to create a primary or secondary site. At this point, you'll continue with a primary site installation. Later in the chapter, you will create a secondary site.

FIGURE 4.11
The Site Type page



- **3.** The next page that appears is the Customer Experience Improvement Program Configuration page, shown in Figure 4.12. Here, Microsoft collects data that aids when it's trying to optimize the product. You can agree to allow data to be sent to Microsoft, or you can decline the option.
- **4.** The Product Key page follows, allowing you to enter the product key for your version of Configuration Manager. This is the same page shown earlier in Figure 4.9.
- 5. When you click Next, you will see the Destination Folder page, as shown in Figure 4.13. You did not have the ability to change the installation directory with the simple setup, but in the custom setup installation, you do. You can either type a new path in the text box or click the Browse button to navigate to the correct path. Once you have entered the path, you can click Next to continue.
- **6.** Just as you did in the simple setup, you can specify the site code and site name on the Site Settings page. This is the same page shown earlier in Figure 4.10.
- Click Next when you have entered the appropriate information, and you will be presented with the Security Mode page.

FIGURE 4.12
The Customer Experience Improvement Program Configuration page

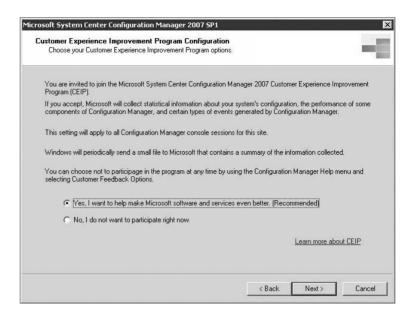
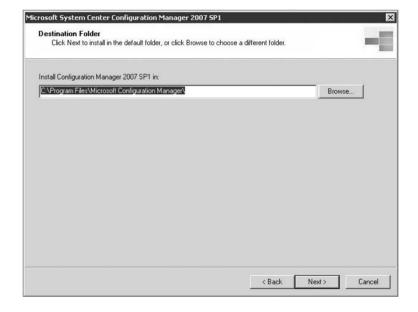


FIGURE 4.13
The Destination
Folder page



- **8.** Click Next to continue.
- **9.** The Client Agent Selection page, shown in Figure 4.14, allows you to enable the client agents that you want to use within your site. All of the available client agents are enabled by default. If you chose to use Mixed mode, you will note that the Network Access Protection option is not enabled. That is because the Network Access Protection service is

not available outside of Native mode. If there are any client agents that you do not want to enable when the site is started up, make sure you deselect them before clicking Next.

FIGURE 4.14
The Client Agent
Selection page



- 10. The Database Server page, shown in Figure 4.15, is used to identify the SQL server and the site database name. By default, the local computer name is listed within the SQL Server and Instance text box, so you will have to change that if your site database is going to reside on a remote SQL Server. The site database name is SMS_sitecode by default. If you decide to make it something else, either to make the name more user-friendly or to follow your organization's naming standards, then you will have to make a change to the ConfigMgr Site Database text field.
- 11. When you move on to the next page, SMS Provider Settings, as shown in Figure 4.16, you can identify the computer that will host the SMS Provider service. By default, the Provider service is installed on the site server for the site, but it does not have to be. You can specify another computer that will host the SMS Provider service, but take note that you cannot host the SMS Provider service on a SQL cluster.
- 12. Next, the Management Point page, shown in Figure 4.17, allows you to install the management point role as you are installing the site server. (Note that SMS 2003 did not give you the option of having the management point available when the site was created. Instead, you would have to define the management point after the initial installation was complete.) On this page you can enter the name of the management point server in the Management Point Computer text box and then click Next to continue.
- **13.** By default, Configuration Manager uses port 80 for communications between the clients and the servers. Once a certificate is installed, you can secure your communications by using HTTPS over port 443. If you want to use different ports, you can override the defaults on the Port Settings page, shown in Figure 4.18.

FIGURE 4.15The Database Server page

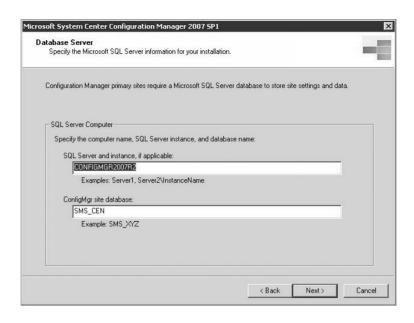
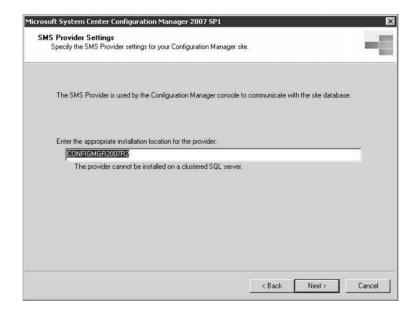


FIGURE 4.16
The SMS Provider
Settings page



14. Once you click Next, you are presented with a Settings Summary page detailing the installation actions that will be performed, as shown in Figure 4.19. Review the settings, and then click Next to start the installation.

FIGURE 4.17The Management Point page

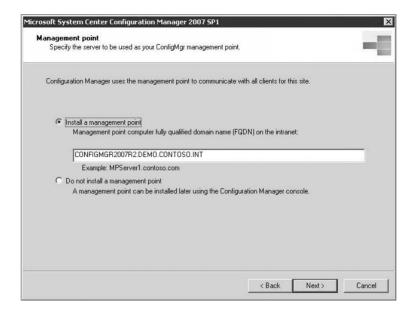
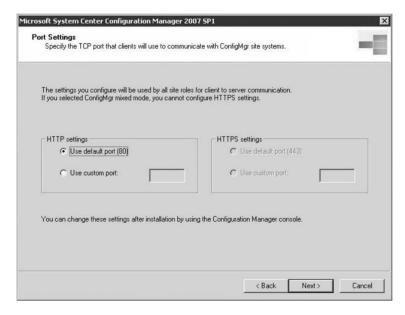


FIGURE 4.18
The Port Settings page



15. A final prerequisite check is performed before installation will occur. As you can see in Figure 4.20, the missing requirements appear, giving you a chance to rectify them. Configuration Manager's installer can resolve some prerequisites, and once you click the Resolve button, it will take care of them. For any that are not resolvable, you will have to fix the problem and then click the Run Check button with this wizard.

FIGURE 4.19
The Settings Summary page

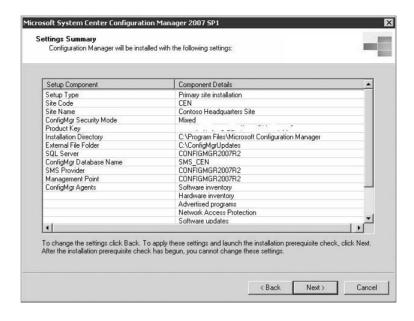
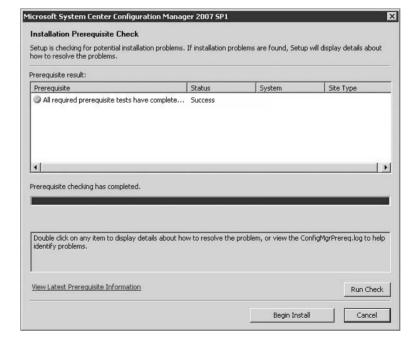


FIGURE 4.20 The final prerequisite check



Unattended Installation

Sometimes you may want to automate the installation of your Configuration Manager site systems. For instance, if you have a remote system and you do not have any administrators located at that site, you can create an *unattended* installation script that will allow you to perform a silent installation. The person who receives the unattended installation file does not need to be familiar with the details of the installation, only how to type in the command that will be used to carry out the setup.

Unlike some of Microsoft's server products, Configuration Manager does not have a utility that will create the unattended file for you. Instead, you will have to use a text editor of some type and create the file manually. However, if you are familiar with the format of unattended files used to install Windows Server or Windows XP products, you will find the unattended installation file for Configuration Manager very familiar.

As in those other products, the unattended file is structured into section names, key names, and values. The sections need to be created, and then each of the keys within the sections will need values configured so that the person performing the install does not have to supply any information to the setup wizard. Once you have the file created, you will need to give it a descriptive name and make sure you include an .ini extension. In our example, the file might be named unattend.ini. Luckily, you don't have to worry about the order of the keys and values within each section, and you don't have to be concerned about the section order. You just need to make sure that the keys are in the right section and the values are valid.

When creating the unattended installation file, you have the following sections and keys to use. Also shown are the possible values for the keys in each section.

The following keys fall into the [Identification] section:

Action Action is a required key that contains three possible values:

InstallprimarySite This value is used when you want to install a primary site.

InstallSecondarySite This value is used when you want to install a secondary site.

InstallAdminUI This value is used when you want to install the Configuration Manager console on a supported system.

The following keys fall into the [Options] section:

ProductID Required 25-digit product key that is used when installing a primary site or the Configuration Manager console.

SiteCode Required three-character site code that is used by all of the site systems as well as the clients when installing a primary or secondary site.

SiteName Required friendly name of the site when installing primary or secondary sites.

ParentSiteCode Required when installing a secondary site or the Configuration Manager console. Used to identify the parent site of the secondary site.

ParentSiteServer Required when installing a secondary site and used to identify the site server in the parent site.

SMSInstallDir Required when installing a primary or secondary site or the Configuration Manager console. This identifies the path where the program files will be installed.

Management Point Optional key that is used when installing a primary or secondary site to identify the computer that will be used as the default management point.

SDKServer Required when installing a primary site and is used to identify the computer that will host the SMS Provider.

ClientAgents Optional key that allows you to designate which client agents will be installed during a primary site installation. The agent types that can be configured are as follows:

SINV Software inventory client agent

HINV Hardware inventory client agent

ADPROG Advertised programs client agent

NAP Network Access Protection client agent

SUM Software update management client agent

SWM Software metering client agent

DCM Desired configuration management client agent

RT Remote tools client agent

SiteSecurityMode Optional key that allows you to specify the security mode that will be used when installing a primary site

Native Used when installing in Native mode. This requires the use of the SiteServerSignCert key:

Mixed Used when installing in Mixed mode.

SiteServerSignCert Required key when the primary site is installed in Native mode. You must include the site server signing certificate thumbprint as the value.

The following keys fall into the [SQLConfigOptions] section:

SQLServerName Required when installing a primary site and used to identify the computer that will host the site database.

CreateSQLDevice Required when installing a primary site and used to specify whether the database should be created during setup. A value of 1 indicates that the database should be configured; 0 indicates that it should not be configured.

Note that the unattended installation can be used only for new installations. If you are upgrading an existing SMS 2003 site, you will not have the luxury of an unattended installation. If you are performing a fresh install, however, you can start the installation by opening a command prompt and navigating to the directory where the setup program is located. Then type the following:

```
setup.exe /script path_to_unnattend_file\unattend.ini
```

You can find additional information on Microsoft TechNet (http://technet.microsoft.com/en-us/library/bb693470.aspx).

These other command-line options allow you to perform upgrades of existing sites, test databases for upgrade, reset site options, and uninstall sites:

/ALLCLIENTOPTIONSON Enables all of the client agents.

/DEINSTALL Uninstalls the site.

/DONTSTARTSITECOMP Installs the site but does not start the Site Component Manager.

/HIDDEN Does not show the setup wizard during installation. This should be used only with the /SCRIPT switch.

/ICPUNATTENDED Installs the International Client Pack.

/NODISKCHECK Specifies that setup will not check disk space requirements when initializing.

/NOUSERINPUT Shows the setup wizard but does not allow user interaction.

/RESETSITE Resets the site database and the service accounts.

/TESTDBUPGRADE Tests the site database to ensure that it is capable of being upgraded. Make sure you run this command on a copy of your database and not the production database, because it can cause corruption of data.

/TRACING:OFF Turns off the logging of setup.

/UPGRADE Performs an unattended upgrade of an existing site. You must supply the product key after the **/upgrade** switch, as follows:

setup /upgrade XXXXX-XXXXX-XXXXX-XXXXX

The final set of command-line switches all check prerequisites before performing an installation. When you use the /PREREQ command, the computer on which you are installing Configuration Manager is checked to make sure that all the prerequisites are in place, and then if you use any of the other switches, the appropriate installation is performed.

/PREREQ Checks the computer for the required software and hardware.

/PRI Installs a primary site after checking that prerequisites are met.

/SEC Installs a secondary site after checking that prerequisites are met.

/MP Specifies the computer that will act as the management point. You must specify the computer name after the /MP switch. This must be used with the /PRI switch.

/SQL Specifies which SQL Server 2005 system will host the site database. You must specify the computer name after the /SQL switch. This must be used with the /PRI switch.

/UI Installs the Configuration Manager console on the computer after checking that the prerequisites are met.

IMPLEMENTING A SECONDARY SITE SERVER

Continuing the System Center Configuration Manager 2007 hierarchy and design scenario from earlier in the chapter, the second server you create will be targeted, installed, and configured as a secondary site server, reporting into the parent Configuration Manager 2007 primary site with a site code of CEN.

- Add the primary site server machine account in the second server's Local Administrators group.
- 2. Open the Configuration Manager 2007 console.
- 3. Expand the Site Management node.
- 4. Right-click the CEN Site node, and select New Secondary Site.
- 5. In the Secondary Site Creation Wizard shown in Figure 4.21, click Next.

FIGURE 4.21 Secondary Site Creation Wizard's Welcome page

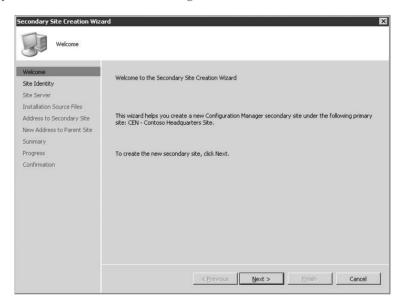
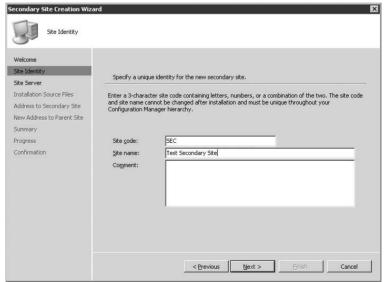
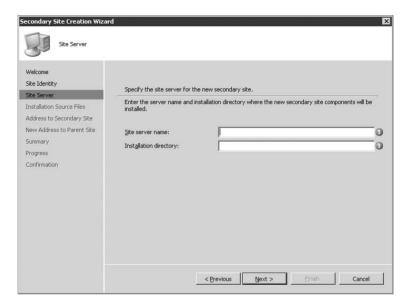


FIGURE 4.22 Site Identity page



- **6.** On the Site Identity page (Figure 4.22), type **SEC** in the Site Code area, type a site name description of **Test Secondary Site**, and click Next.
- **7.** On the Site Server page (Figure 4.23), type the second server's NetBIOS name in the Site Server Name field, type the installation directory (for example, **d:\Program Files\ConfgMgr2007**) in the Installation Directory, and click Next.

FIGURE 4.23 Site Server page



- **8.** On the Installation Source Files page (Figure 4.24), accept the default of Copy Installation Source Files Over The Network From The Parent Site Server, and click Next.
- **9.** On the Address to Secondary Site page (Figure 4.25), accept the default Yes. Create A New Address radio button, and click Next.
- **10.** Click Next on the next two pages.
- **11.** Review the Summary Details page, and click Next.
- 12. Click Close.

TROUBLESHOOTING A CONFIGURATION MANAGER 2007 SITE SERVER

To validate that a site server is functioning properly, you should review the smsexec.log file. The SMS Executive service is the main service of Configuration Manager 2007. This log will show each thread or subcomponent of the service and log the status of whether it has started successfully. The smsexec.log, as shown in Figure 4.26, is one of the initial places an administrator can review to gain insights into how the site server may be running.

Site Database Server

Every Configuration Manager 2007 implementation will have at least one server running the site database server role. The simplest implementation will have a single server running all

the Configuration Manager 2007 roles as well as Microsoft SQL Server 2005 Service Pack 2. As noted earlier, at least one database repository is required to store all the client information as well as site configurations.

FIGURE 4.24 Installation Source Files page

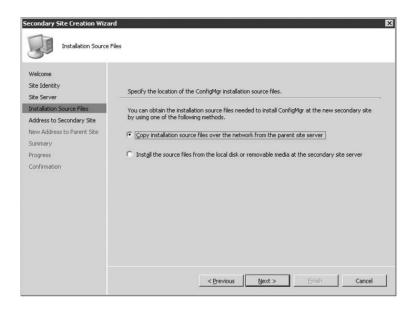


FIGURE 4.25Address to Secondary Site page

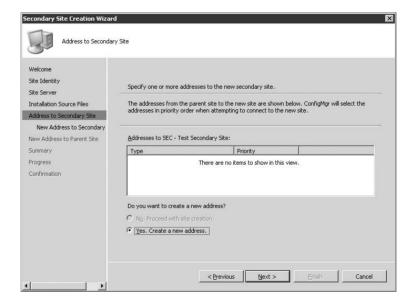
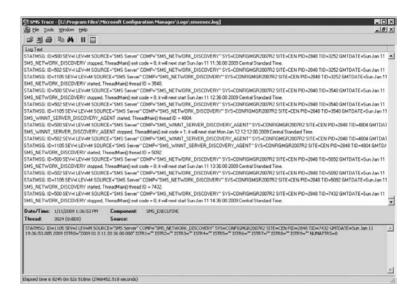


FIGURE 4.26
Reviewing smsexec.log



SOFTWARE REQUIREMENTS

A Configuration Manager 2007 site database server requires the following:

- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- ◆ SQL Server 2005 Service Pack 2 is the only version of SQL Server supported for hosting the Configuration Manager 2007 site database.
- The SQL database service is the only SQL Server component required to be installed to host the site database.

TROUBLESHOOTING A CONFIGURATION MANAGER SITE DATABASE SERVER

This is the database server that hosts the SQL Server 2005 Service Pack 2 or higher database. There is one database that holds all information about inventory, packages, status, and all the other pertinent data of System Center Configuration Manager 2007. The following logs provide insight into the health of the database server:

smsdbmon.log This log shows all database activities such as inserts, updates, drops, and deletes from the Configuration Manager 2007 database.

smsprov.log This log shows the SQL transaction calls made from the Configuration Manager console or automation scripts via the SDK.

Site Server Roles

Most organizations that are taking advantage of Configuration Manager will create multiple sites so that they can control the client traffic or manage administrative control. Primary sites can act as a parent site to primary or secondary sites. Secondary sites cannot be a parent site; they can only be child sites beneath an existing primary site. You deploy multiple Configuration Manager

2007 sites to create a hierarchical structure that allows administrators from parent sites to have administrative control over the child sites.

Plan the order in which you will deploy and attach sites, thereby creating data flow between the sites in a hierarchy branch. Attaching secondary sites is easy; all you have to do is install the secondary site, which requires that you have the primary site already installed. The site communication between a secondary site and its parent primary site is configured during secondary site installation.

Creating a hierarchy with multiple primary sites is a little more difficult. After installing primary sites, you must configure the appropriate site server roles. Site server roles support the various features of the product that you're looking to implement.

The following site server roles can be configured:

- ♦ SMS Provider
- Component server
- Distribution point
- ◆ Fallback status point
- Management point
- PXE service point
- Reporting point
- Server locator point
- Software update point
- State migration point
- System health validator point

HOW MANY PHYSICAL SERVERS?

Do not be afraid of the number of site server roles described in this chapter. Some Configuration Manager shops will deploy one or two servers that host all of the appropriate site server roles. Just remember to plan and size accordingly.

SMS Provider

Within Configuration Manager 2007, the Configuration Manager console does not access the database directly. It leverages the SMS Provider role, which consists of Windows Management Instrumentation (WMI) layers and conducts the read and write operations to the Configuration Manager 2007 database. The SMS Provider role also ensures that the appropriate security is maintained as provisioned within the Configuration Manager 2007 console.

SMS Provider Namespaces

An architected schema has been put in place in order to provide consistent access to WMI. The namespaces are frequently leveraged when attempting to automate or troubleshoot Configuration Manager 2007, as shown in Table 4.1.

TABLE 4.1:	SMS	Provider	Namespaces
-------------------	-----	----------	------------

NAMESPACE	DESCRIPTION
root\SMS\site_ <sitecode></sitecode>	This is the WMI namespace for the SMS Provider role leveraged by the Configuration Manager 2007 console, Resource Explorer, tools, and scripts.
root\SMS\SMS_ProviderLocation	This WMI namespace provides the SMS Provider role for a given Configuration Manager site.
root\CIMv2\SMS	This is the WMI namespace that is leveraged heavily to access hardware and software inventory information that is enabled in the sms_def.mof file.
root\CCM	This is the WMI namespace for client configuration policy and client data.

Software Requirements

In Configuration Manager 2007, the SMS Provider role requires the following:

- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- ◆ The SMS Provider role must be installed on a computer in the same domain as the site server and site database server site systems.
- The SMS Provider role cannot be installed on a virtual SQL Server cluster computer or a physical computer hosting a virtual SQL Server cluster node.
- The SMS Provider role cannot be installed on a computer already hosting the SMS Provider role for another site.

Troubleshooting a Configuration Manager SMS Provider

The SMS Provider role provides insights into how the Configuration Manager console creates calls to the Configuration Manager 2007 database. This becomes helpful when you start to script, automate, and customize Configuration Manager. The smsprov.log file documents the WMI/SQL calls within Configuration Manager (see Figure 4.27). Specifically, it documents the times, dates, user, and WQL/SQL that is being executed. This log lends great insights into the Transact-SQL queries being performed on the Configuration Manager database. These can be leveraged later if you plan on doing some customization for reports, collections, or other activities that might require querying the database.

COMPONENT SERVER

A *component server* is any server that is running the SMS Executive service within the hierarchy. This service runs specified threads that support other roles such as a management point, server locator point, or the like, thus potentially reducing the overhead on a site server. The only role that is not a component server is the distribution point role.

FIGURE 4.27
A sample smsprov.log



Troubleshooting a Configuration Manager Component Server

This role manages the threads of the SMS Executive service. It maintains which roles are local and remote for a given site. The following logs may be reviewed to gain insights into the component server health:

sitecomp.log This log shows all the site roles and where they're configured to be running. **compmon.log** This log records the status of all the threads of the SMSExec.

DISTRIBUTION POINT

A *distribution point* is nothing more than a "glorified file server." Its role is to store the software packages to be delivered to the clients. Over the years, this role has developed into a more sophisticated file server than the original distribution points. Several delivery mechanisms and configurations make the Configuration Manager 2007 distribution point highly effective and scalable.

A few strategies and configuration options may be leveraged with distribution points. From a core level, clients may run the software installation routines remotely over the Server Message Block (SMB) protocol. If the distribution point is running and configured to use Internet Information Services (IIS), the client architecture can leverage the Background Intelligent Transfer Service (BITS) over an HTTP or HTTPS protocol. Lastly, a distribution point can be designated as a protected site system. This enables the administrator to service a designated set of clients without the potential impact on the WAN of servicing clients from a different physical site.

THE COPY PACKAGE FUNCTION

One of the new features within Configuration Manager 2007 is the Copy Package function. You can use Copy Package to roll out new distribution points or branch distribution points by using either the Packages node or a list to select the packages to send as well as the source and destination distribution points.

There are three types of distribution points:

- Distribution point
- Protected distribution point
- Branch distribution point

What these have in common is the fundamental role of the distribution point: to store software packages as close to the endpoint clients as possible and to present those packages, either by the clients downloading via BITS or running them off the server via SMB, to the clients it is serving.

The Branch Distribution Point

Another struggle that organizations have had over the years has been supporting remote locations. In fact, most organizations are attempting to move servers out of remote locations. These locations typically did not have a secure, well-ventilated room to store infrastructure hardware effectively. In some scenarios, they were also connected over slower links than typically needed to support the number of endpoint-managed clients at that location. Thus, attempting to support these locations in prior versions of SMS proved to be quite challenging. Microsoft intends to address this business challenge by a feature called the *branch distribution point*.

The branch distribution point was introduced to address smaller locations (those with 2 to 100 managed clients) or locations with low bandwidth where client management is needed. The branch distribution point has similar capabilities to a distribution point with subtle differences. The first and most apparent difference is that a branch distribution point runs on the workstation operating system (Windows XP Service Pack 2 and higher) as well as the server operating system (Windows Sever 2003 Service Pack 1 and higher). Another feature of the branch distribution point is that it leverages BITS in order to download the targeted package across the WAN. The software can reach a branch distribution point in two different ways: a targeted distribution or an on-demand request.

Targeted distributions are identical to how distribution points are leveraged. Once a package is created, the distribution points may be selected. That selection can be a standard distribution point or a branch distribution point.

Note that a branch distribution point cannot be a distribution point for Internet-based clients, because the client protocol that pulls down packages from the branch distribution point to the client is SMB.

The "on-demand" package allows the branch distribution point to accept a request from a client that is requesting a package that is not present. If the package properties include "Automatically download content when packages are assigned to a branch distribution point," as in Figure 4.28, the branch distribution point will automatically download the package and service the request.

Architectural design considerations must be thought through before implementing the branch distribution point scenarios. For example, having a single branch distribution point for 20 managed clients hosted on Windows XP Service Pack 2 will have a potential impact on software delivery timing, because of the limit, built into the operating system, of 10 incoming connections. The remaining clients will be put into a retry state for package source location until there are open connections. The on-demand scenario, although flexible, can potentially impact WAN performance if packages are being downloaded unexpectedly.

Protected Site as a Distribution Point

When a server is specified to act as a distribution point site system, you can also enable the distribution point as a *protected* site distribution point. This allows the administrator to specify site boundaries; a client must be within the boundary to utilize the distribution point for package source files. You can select only those boundaries that are already configured for the site. This

gives the administrator more control over which clients use specific distribution points. This setting is recommended for dial-up RAS solutions to make sure all RAS clients use a specific DP, which ideally would be the closest distribution point.

FIGURE 4.28
Package properties for branch distribution point

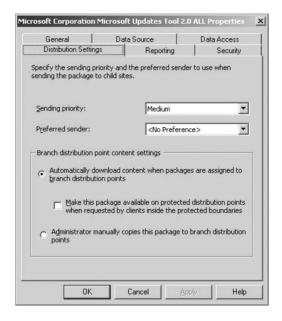
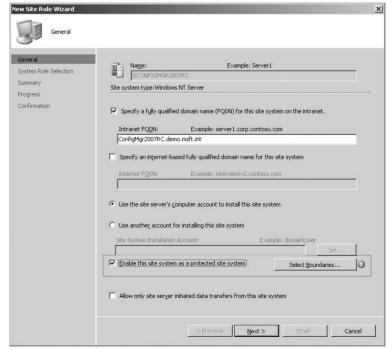


FIGURE 4.29
Enabling a Protected
Site window



As an example, let's say there is a single site with 5,000 clients. There are three distribution points enabled for the site. You could allow the clients to randomly select an available distribution point, but this might allow clients to overload a single distribution point. The protected distribution point setting allows you to balance the load by selecting available site boundaries for specific distribution point servers. Figure 4.29 illustrates how to enable a Protected Site.

Space Recommendations and Scalability for the Distribution Point Role

Disk space is the most important consideration when planning the capacity of a distribution point. Another consideration will be the network connection of the server and how it will service its designated clients. Consider the following points when sizing your distribution points:

- When Configuration Manager 2007 utilizes the source files directly during a software distribution and is performing the distribution point role, the site server requires disk space equal to the package size.
- When sending packages to child sites, the site server needs to have additional disk space of half the size of the original package size.
- When storing a compressed version of the source files, the site server needs to have additional disk space of 1.5 times the size of the original package size.

Targeted distribution points need to have disk space equaling 1.1 times the size of the original package. The additional tenth is utilized for the binary delta replication information for each package.

Scalability and redundancy are other architectural decisions that you should not take lightly. You may have the most highly available infrastructure, but if you cannot service managed clients, it will be all for naught. To that end, even some of the smallest Configuration Manager 2007 hierarchies should have at least two distribution points. This allows for site failure while still allowing clients to remain being managed. Within some of the largest infrastructures, architects must also take into account that a single distribution point can service approximately 4,000 clients (taking into account adequate hardware and sufficient network connections). That does imply that if you are managing 12,000 clients that the hierarchy needs only three distribution points. We usually recommend that our customers scale their distribution points to 2,000 clients; thus, during failover, the maximum scale potentially could be met. It cannot be overstated that a solid disk subsystem and network throughput are essential for scaling a distribution point.

Software Requirements

Configuration Manager 2007 distribution points require the following:

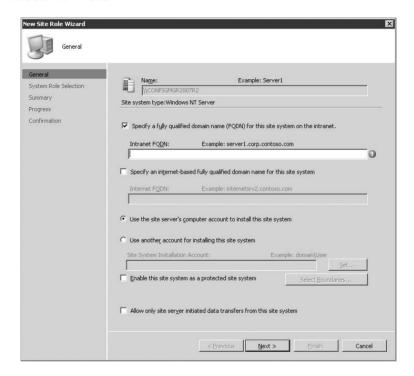
- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- They must be Background Intelligent Transfer Service (BITS)—enabled distribution points. This role requires BITS server extensions and Web Distributed Authoring and Versioning (WebDAV) extensions. IIS is not required if the distribution point will not be BITS-enabled.
- All Configuration Manager distribution point systems using BITS bandwidth throttling require BITS 2 or higher.

Implementing the Distribution Point Role

Take the following steps to implement the distribution point role on a server:

- 1. Open the Configuration Manager 2007 console.
- **2.** Expand the Site Management node by selecting CEN ➤ Site Settings ➤ Site Systems.
- **3.** On the General page of the New Site Role Wizard (Figure 4.30), right-click the primary site server name, and select New Roles.

FIGURE 4.30
The New Site Role
Wizard



- 4. In the New Site Role Wizard, click Next.
- On the System Role Selection page (Figure 4.31), under Available Roles, select Distribution Point, and click Next.
- 6. Review the Summary Details page, and click Next.
- Click Close.

Troubleshooting a Configuration Manager 2007 Distribution Point

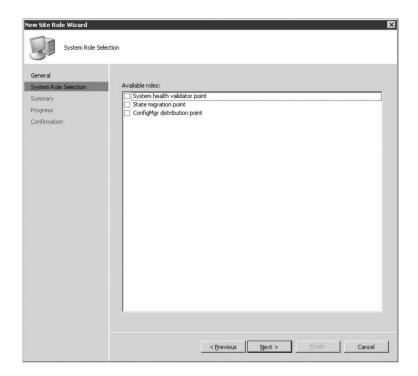
Without the packages being staged on the distribution points, both standard and/or branch, software distribution cannot be completed. Providing insights into the process and health of the hierarchy distribution points, log files can be an administrator's best friend.

The following logs provide insights into the distribution points for troubleshooting purposes:

distmgr.log This log tracks the different packages, by package ID, size, and location where they are to be stored.

Branch Distribution Point on Client System (PeerDPAgent. log) This log will show whether the client is a branch distribution point and its package download status.

FIGURE 4.31Selecting the distribution point role



FALLBACK STATUS POINT

The fallback status point role is new in Configuration Manager 2007, added to address today's greater security requirements while enabling a mechanism to catch clients that are not communicating properly. When Configuration Manager 2007 is configured in Native mode, it requires client certificates. This requirement can potentially deny a managed client access if the certificate becomes damaged or corrupted. If a managed client could not communicate with the hierarchy, it would eventually become orphaned, leaving it in a potentially unmanaged state. The fallback status point role provides an administrator with insight into the installation and management of a client.

A *fallback status point* is similar to a proxy server that proxies client status messages up to the site server. Two types of messages may occur: the normal messages that appear during client installation and assignment or those identifying unhealthy Configuration Manager 2007 clients. In either scenario, the fallback status point fills the gap and shows the administrator that there are client issues that need to be addressed.

Because of the potential security threat of an unknown client or client status, it is recommended that the fallback status point be placed outside a physical site server. It can be a low-end server, because of the relatively small number of potential requests it should receive. As in any design decision, the criteria of scale vs. risk should be investigated before a decision is made.

Through detailed reporting, an administrator can gain impending knowledge and take proactive measures to ensure that availability remains in its highest state. These reports include detailed client information on capable and incapable client communication.

Software Requirements

Configuration Manager 2007 fallback status points require the following:

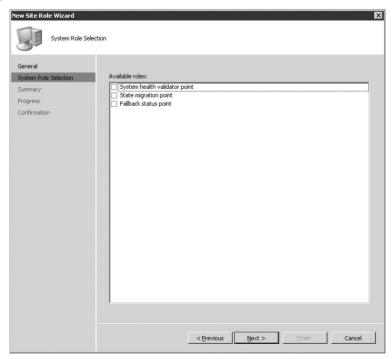
 All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.

Implementing the Fallback Status Point Role

Take the following steps to implement the fallback status point role on a server:

- 1. Open the Configuration Manager 2007 console.
- **2.** Expand the Site Management node by selecting CEN ➤ Site Settings ➤ Site Systems.
- 3. Right-click the primary site server name, and select New Roles.
- 4. In the New Site Role Wizard, click Next.
- On the System Role Selection page (Figure 4.32), under Available Roles, select the Fallback Status Point box, and click Next.

FIGURE 4.32Selecting the fallback status point role



- **6.** Review the Summary Details page, and click Next.
- 7. Select Close.

Troubleshooting the Fallback Status Point

The fallback status point is meant for clients that are having difficulties communicating with a Native mode Configuration Manager hierarchy. To provide insights into the proper configuration of this role, the following logs are needed:

SMSFSPSetup.log This log documents the prerequisites and kicks off the fsp.msi installation.

fspMSI.log This log provides the installation status of the fallback status point role.

MANAGEMENT POINT

The management point role is another site system role within Configuration Manager 2007. A *management point* is the primary point of contact between the Configuration Manager 2007 clients and the site server. Management points serve clients in much the same way that they did in SMS 2003. Since this was a major architecture shift from SMS 2.0 to 2003, there was not a need to do a lot of focused work on this solid infrastructure piece for Configuration Manager 2007.

Configuration Manager 2007 clients communicate with sites through management points. To hold the role of a management point, the server must have IIS installed, enabled, and correctly configured. Additionally, the following considerations should be taken into account:

- ◆ Every site must have a default management point specified.
- Management points can be set to use the SMS site database or a replicated copy of the SMS site database.
- Management points can be a single physical server or a single virtual server (multiple physical servers) that is accessed via a network load balancing (NLB) cluster.

Management Point Functions

A Configuration Manager site should have only one default management point. Configuration Manager clients communicate only with the default management point. If additional management points are needed for performance reasons or redundancy, combine multiple management points of one site into an NLB cluster and configure the virtual IP address of the cluster as the default management point for that site.

A management point does the following:

- It provides specific client configuration details to the Configuration Manager client after installation.
- ◆ It uses the sms_def.mof file that is stored in the site database to create the appropriate Configuration Manager client policy for Configuration Manager clients.
- Configuration Manager clients retrieve client policies from the management points.
- The Configuration Manager client stores retrieved policies locally in WMI in the form of instances and classes.
- It serves as the location where Configuration Manager client computers check for advertisements.

- It locates distribution points for Configuration Manager clients. Clients choose a distribution point at random from the list of available distribution points provided by the resident management point when making package source file requests.
- It receives inventory, software metering, and status information from the Configuration Manager clients and forwards the information to the site server.

Proxy Management Points

When traversing the WAN, normal Configuration Manager client operations may consume large portions of the available network bandwidth. To reduce WAN traffic, you can deploy *proxy management points* at secondary sites.

The Configuration Manager client uses a proxy management point when it is within the site boundaries of a secondary child site. To use a particular secondary site's proxy management point, the configuration client must be assigned to that secondary site's parent site.

Proxy management points can significantly reduce the load on the WAN traffic by processing data from and providing client policy to those clients that fall within their roaming boundaries. Data flows between Configuration Manager clients and the Configuration Manager 2007 hierarchy is as follows:

- Clients send discovery data, inventory data, status data, and software metering data to the proxy management point in XML format.
- 2. The proxy management point processes the submitted XML file, converts it into the appropriate file type, and places it in the associated Inbox directory on the secondary site server.
- The secondary site server processes the data as it would under normal circumstances and forwards it up the hierarchy as appropriate.

Proxy management points also retrieve policy information from the database of the primary site and forward the data to Configuration Manager clients. Proxy management points allow the client to function locally when roaming to a secondary site, while further allowing administrators to control the replication of client data from the secondary site to the primary parent by means of standard sender throttling.

The first key benefit of deploying a proxy management point (on a secondary site) is in the network traffic- and network-scheduling capabilities that the secondary site provides when sending inventory data files up the hierarchy.

Without a proxy management point at a location, the Configuration Manager client will send all its inventory data over the WAN to a management point over the WAN; this is based on the client inventory schedule. The client has the ability to marginally compress the data, but it is realistically optimized for speed. Conversely, the secondary site server is optimized for file size.

With a proxy management point at the location, the client will send inventory files. Once they are received, the proxy management point will convert them from XML to native Configuration Manager file formats and "forward" them to the secondary site. The secondary site will then compress these files and forward them, via the sender (and using the sender scheduling and bandwidth controls), to its parent primary site server. The secondary site will also send these files in batches (saving even more space) on a per-file-type basis, if there are multiple inventory files of the same type.

For locations with a small number of clients, the difference between having a proxy management point and not having one is very small, because a secondary site server sender header adds overhead for network traffic that could cause more traffic than not having one at all. However, as the number of clients at that location grows, so too does the network savings. This is potentially where a proxy management point can be leveraged.

Server Load Balancing

Management points can also utilize NLB clusters. When all management points for a site are combined into a Windows NLB cluster, Configuration Manager clients resolve the IP address of the cluster, thus balancing client load between multiple management points in a large infrastructure.

How Advanced Clients Find Management Points

During installation and general operation, Configuration Manager 2007 clients obtain site assignment and management point locations from the Active Directory global catalog or WINS. If a machine does not resolve a management point for some reason, a request to the server locator point may potentially occur.

Locating Management Points in AD

In an environment that provides Active Directory services, Configuration Manager 2007 clients locate management points as follows:

- The client searches the Active Directory global catalog for a local site code with a matching Active Directory site name, IP network, or IP address range that has been previously registered by a site server.
- 2. If a match is not found or if required content is not available at the local site, then the client uses the site code of its assigned site.
- **3.** The client then queries Active Directory again to find the appropriate management point for the site code identified in the previous steps. For this reason, management points should be installed prior to Configuration Manager client deployment, but the client will be able to access the management point once it becomes available.
- **4.** If there is only one management point for the site, the client gets the name of that management point from Active Directory and then connects to it.

Locating Management Points in WINS

In an environment without Active Directory, Configuration Manager 2007 clients attempt to locate a management point through WINS. Management points are usually registered in WINS automatically during management point installation. This allows clients to perform a WINS lookup based on site code and obtain a management point IP address. When querying WINS for the location of a management point, the client searches for the 1A entry named MP_Sitecode.

Automatic MP Query

When installing the Configuration Manager client, either set it to determine the SMS site automatically or specify site assignment as part of the command line for the installation. Once installed and assigned to a site, the client begins using the default management point for that site. If it is not assigned to a site automatically, or via the use of command-line switches, it will attempt to determine site assignment every 25 hours until it becomes assigned. Once the Configuration Manager client is assigned to a site, it checks every 25 hours (during the client refresh cycle) to verify that the default management point for the assigned site has not changed. If the default management point has changed, the Configuration Manager client will begin using the new default management point. You can see this in the LocationServices.Log file of the Configuration Manager client, located at %Windir%\System32\CCM\Logs.

Logging

Logs of management point activity can exist in one of two locations, depending upon which was installed first, the Configuration Manager client or the management point. If the management point is installed on a server first, the logs will be located in the SMS_CCM\Logs directory. When the Configuration Manager client has already been installed on the server, the logs are located in the Windir%\System32\CCM\Logs directory along with the client-side logs.

Software Requirements

Configuration Manager 2007 management points require the following:

- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- ◆ IIS 6.0 or higher must be installed.
- ◆ BITS server IIS extensions and WebDAV IIS extensions must be installed.

Implementing the Management Point Role

Take the following steps to implement the Management Point role on a server:

- 1. Open the Configuration Manager 2007 console.
- 2. Expand the Site Management node.
- **3.** Expand the CEN node, and choose Site Settings ➤ Site Systems.
- 4. Right-click the primary site server name, and select New Roles.
- 5. In the New Site Role Wizard, click Next.
- **6.** On the System Role Selection page (Figure 4.33), under Available Roles, select the Management Point box, and click Next.
- **7.** Review the Management Point details page (Figure 4.34), and click Next.
- 8. Click Close.
- Review the rsetup.log file on the primary site server logs directory for "Installation was successful."

Troubleshooting a Configuration Manager 2007 Management Point

The Configuration Manager management point is the entry point into a Configuration Manager hierarchy from a client perspective. The client receives its Configuration Manager policies and advertisements from the MP and places its inventories and status there. Use the following logs for troubleshooting:

mpMSI.log This log is the Microsoft Installer (MSI) log for the management point installation.

mpSetup.log This is the site-specific management point log, which shows which site and server the management point is configured to use.

mpcontrol.log This log maintains the management point by reviewing and checking the management point availability and status.

FIGURE 4.33 Selecting the management point role

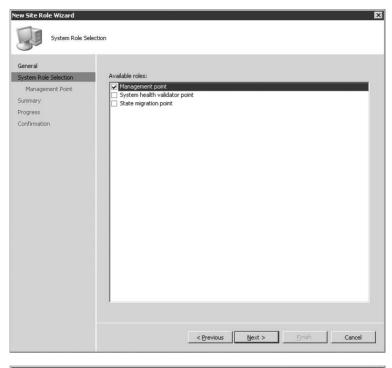
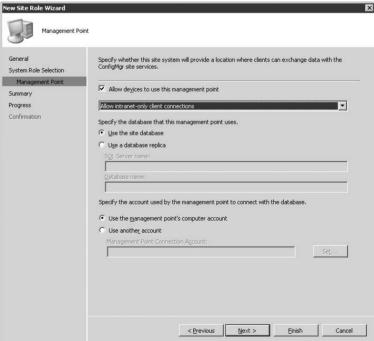


FIGURE 4.34
The Management Point details page



PXE SERVICE POINT

The *PXE service point* site system responds to and initiates operating system deployments from computers whose network interface cards are configured to allow PXE boot requests. The PXE service point provides integration with the Windows Deployment Services (WDS) server role, which allows it to be managed by Configuration Manager as a site role. WDS hosts multiple providers, and Configuration Manager puts itself first. When a client PXE boots and checks with WDS, WDS checks with Configuration Manager first. If the client is known by Configuration Manager, it passes the WinPE boot image for use. Otherwise, WDS falls through to the next provider.

Software Requirements

Configuration Manager 2007 PXE service points require the following:

- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- A WDS server must be installed and configured. The key configuration item is that WDS does not respond to client requests.

Implementing the PXE Service Point Role

Take the following steps to implement the PXE service point role on a server:

- **1.** Open the Configuration Manager 2007 console.
- 2. Expand the Site Management node.
- **3.** Expand the CEN node, and choose Site Settings ➤ Site Systems.
- 4. Right-click the primary site server name, and select New Roles.
- 5. In the New Site Role Wizard, click Next.
- **6.** On the System Role Selection page (Figure 4.35), under Available Roles, select the PXE Service Point box, and click Next.
- **7.** The warning box shown in Figure 4.36 may appear. Click Yes.
- **8.** Enable unknown computer support. Enabling this setting prompts the warning dialog box shown in Figure 4.37. Click OK.
- **9.** On the PXE General page (shown in Figure 4.38), provide a password for computers that boot to PXE, and click Next.
- Determine a suitable account to be used by the PXE service point to connect with the database, and click Next.
- **11.** Review the Summary Details page, and select Next.
- 12. Select Close.

Troubleshooting a Configuration Manager 2007 PXE Service Point

This role is used to initiate the operating system deployment process through a preexecution state. To maintain and troubleshoot this role, you must review the PXESetup.log file. This log documents the needed prerequisites and connections to the WDS server.

FIGURE 4.35
Selecting the PXE service point role

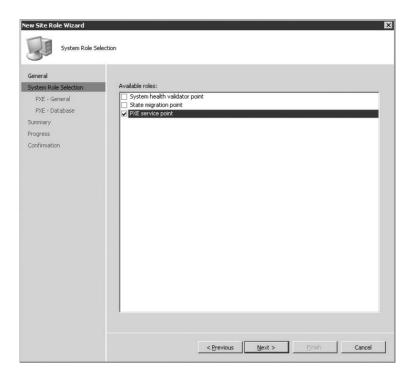


FIGURE 4.36PXE service point configuration warning



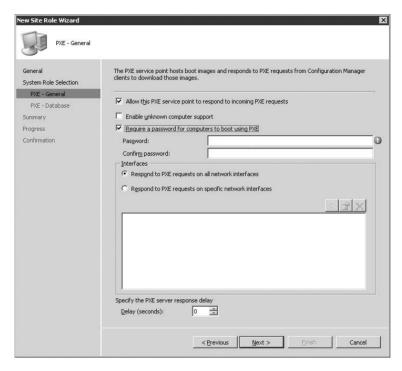
FIGURE 4.37 Unknown computer support warning



REPORTING POINT

The reporting features of Configuration Manager 2007, discussed in detail in Chapter 11, allow you to display site information by retrieving specific data from the SMS site database and displaying it in an easy-to-read format in a web browser. Two types of reporting can be implemented within the context of a reporting point: the legacy web reporting and Configuration Manager leveraging SQL Reporting Services (SRS). SQL Reporting Services was introduced in Configuration Manager 2007 R2. SRS is the strategic direction of reporting with the System Center family. This decision provides your organization with an enterprise-class reporting engine as well as all the feature sets that SRS provides.

FIGURE 4.38PXE Service Point general settings



Reports are Configuration Manager objects that define specific report properties. Currently more than 350 reports ship with Configuration Manager 2007, in the following categories:

- Asset intelligence (70 reports)
- Client status (6 reports)
- Desired configuration management (25 reports)
- ◆ Device management (18 reports)
- Driver management (13 reports)
- Hardware (39 reports)
 - CD-ROM (4 reports)
 - Disk (8 reports)
 - ◆ General (2 reports)
 - Memory (5 reports)
 - Modem (3 reports)
 - ♦ Network adapter (3 reports)
 - Processor (5 reports)
 - ◆ SCSI (3 reports)

- Sound card (3 reports)
- ◆ Video card (3 reports)
- ◆ Network (6 reports)
- Network access protection (13 reports)
- Operating system (9 reports)
- ◆ SMS site (36 reports)
 - ◆ Client information (21 reports)
 - ◆ Discovery and inventory information (10 reports)
 - ◆ General (2 reports)
 - ◆ Server information (3 reports)
- Software (16 reports)
 - ◆ Companies and products (11 reports)
 - ◆ Files (5 reports)
- ◆ Software distribution (24 reports)
 - ◆ Advertisement status (8 reports)
 - ◆ Advertisements (4 reports)
 - ◆ Collections (3 reports)
 - ◆ Packages (9 reports)
- ◆ Software metering (13 reports)
- ◆ Software updates (34 reports)
 - ◆ Compliance (9 reports)
 - ◆ Deployment management (8 reports)
 - Deployment states (7 reports)
 - ♦ Scan (4 reports)
 - ◆ Troubleshooting (4 reports)
 - ◆ Distribution status for SMS 2003 clients (2 reports)
- State migration (3 reports)
- ◆ Status messages (12 reports)
- ◆ Status messages Audit (4 reports)
- ◆ Task sequence (28 reports)
 - ◆ Advertisement status (11 reports)
 - ◆ Advertisements (11 reports)

- ◆ Progress (5 reports)
- ◆ References (1 report)
- Upgrade assessment (6 reports)
 - Windows Vista (4 reports)
 - ◆ Windows XP (2 reports)
- Users (3 reports)
- Virtual Applications (7 reports)
- ♦ Wake on LAN (5 reports)

All of these reports can be copied and manipulated to a specific data set in which you are interested. As discussed in Chapter 11, you can clone a report to modify it where needed.

Default and Custom Reports

You can combine SMS data classes in SQL views to create reports. All reports are created, configured, and managed through the Configuration Manager console. Reports can be displayed in Internet Explorer 5.01 Service Pack 2 or higher. The default reports provided with Configuration Manager 2007 can be used to display status messages, inventory data, and other information about your site or hierarchy.

You can create custom reports to display other information required for your organization. Custom reports can be formatted as HTML files, text files, Active Server Pages, or any other format that can be displayed in a browser. To create custom reports, you should have a basic understanding of SQL and underlying SMS data classes specified in SQL views that make up a report. Each SQL view provides specific information. Multiple SQL views may be combined to generate complex reports.

Another feature within a Configuration Manager report is the ability to refresh the data within a report automatically. This may be useful when a report uses more resources when run or refreshing on the administrator's schedule rather than a report operator.

Dashboards

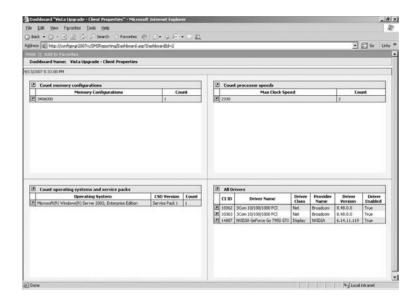
Dashboards have been carried over from SMS 2003. They are sets of reports laid out in a grid format in a single window of Report Viewer. With this feature, you can use a single dashboard to monitor a variety of information about your Configuration Manager site without the need to flip through multiple reports.

For example, if your organization is going through an upgrade from your current operating system to Windows Vista, you can create a dashboard with four reports. As shown in Figure 4.39, a dashboard might include attributes such as processor, memory, operating systems, and drivers.

How Reporting Works

When a server is designated as a reporting point, IIS services on the reporting point are configured to provide a reporting virtual directory (typically http://<servername>\smsreporting_<Site Code>). This site can leverage HTTPS port 443 by default, as well as customizing the given URL.

FIGURE 4.39
A dashboard of client attributes for an upgrade to Vista



Launching a Report

The Reporting node of the Configuration Manager console allows you to manage and view SMS reports. To access the Reporting node, follow these steps:

- 1. Open the Configuration Manager console.
- 2. Navigate to the Site Database ➤ Computer Management ➤ Reporting ➤ Reports node.
- **3.** Right-click the desired report.
- **4.** Select All Tasks ➤ Run to display the report in a web browser.

You can also connect directly to the report by entering the designated URL in the Internet Explorer Address box.

Viewing Reports

As noted, all reports are Configuration Manager 2007 objects; this implies that each object is able to have security tied to it. To that end, you can give users or security groups the ability to see all reports, a subset, or just a single report. Security can be set at the individual report instances or on the entire class of all reports. Reports are categorized to help users locate specific information quickly. When a user runs a report, the SQL statement defined for the report accesses read-only SQL Server views instead of the actual tables of the SMS database and returns the formatted results in an Internet Explorer window.

PLANNING REPORTING POINT

Reporting points communicate with the local SMS site database server and use SQL views to generate the reports. For this reason, they can exist for primary site servers. Depending on the

administrative structure in place, you may need only one reporting point, or your organization might decide to roll out regionalized reporting points so that regional administrators have a view of their assets.

Locations

The location of reporting points in your infrastructure depends on the data required to generate reports. For example, a reporting point should be located at the central site of your Configuration Manager hierarchy for reports that include data from all sites.

If you plan to utilize reports specific to software distribution or software metering data, you should assign the reporting point roles for sites to which those clients report. Reports on software distribution success and/or failure capture only the data for clients of that particular site. Software metering data is summarized before transmittal to the parent site, so reports on software metering that are not run at the assigned site will reflect this summarization only.

Load Balancing

Larger Configuration Manager infrastructures with a multitude of report users and in need of additional scalability should consider planning for multiple reporting points. This allows you to provide different reporting point access URLs to different sets of users. However, you should be aware of the possibility that the performance of your Configuration Manager site database server may be degraded if report and query use is very high. This is especially true if a large number of users are using the same reporting query. You may also want to consider the security needs of your environment and the need to secure not only the server itself but the individual reports as well.

Custom Reports

In addition to planning the location of your reporting points, you should consider whether you will be using the predefined reports alone or whether you will create custom, supplemental reports. These supplemental reports can provide your company with the flexibility of additional reporting options. Should you decide to create custom reports, make sure that staff members who are creating the reports have the appropriate programming skills and that sufficient documentation exists to build security into those reports.

Software Requirements

Configuration Manager 2007 reporting points require the following:

- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- This role requires Active Server pages.
- ◆ Internet Information Services (IIS) 6.0 or higher is required.
- SQL Server access to the SMS database.

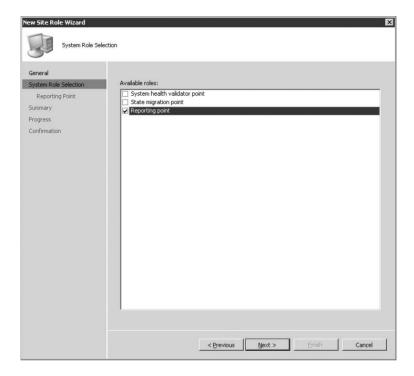
Implementing the Reporting Point Role

Take the following steps to implement the reporting point role on a server:

- **1.** Open the Configuration Manager 2007 console.
- **2.** Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.

- **3.** Right-click the primary site server name, and select New Roles.
- 4. In the New Site Role Wizard, and click Next.
- On the System Role Selection page (Figure 4.40), under Available Roles, select the Reporting Point box, and click Next.

FIGURE 4.40 Selecting the reporting point role



- **6.** Review the Summary Details page, and then click Next and Close.
- 7. Review the rsetup.log file on the primary site server logs directory for "Return 0" and "Finished."
- **8.** Review the SMSReportingInstall.log file for "Installation of Reporting Point Complete."

Troubleshooting a Configuration Manager 2007 Reporting Point

It could be argued that a reporting point isn't essential to a Configuration Manager setup. But if you don't install a Reporting Point, you're receiving all of this robust data from all of the clients in the enterprise yet not able to gain insights into them without a reporting point. To ensure that this role is set up and functioning properly, you should review the following logs:

rsetup.log This is the reporting point setup log, recording the process of enabling the role. **smsreportinginstall.log** This is a supplemental installation log of once the process has kicked off and completed.

smsreporting.log For each report, this log records which user ran the report and shows the associated SQL statement that populates the report.

SERVER LOCATOR POINT

Server locator points (SLPs) are used within a Configuration Manager 2007 hierarchy to provide client services for site assignment, location of client installation files, and location of a management point when clients cannot access that information within Active Directory. Additionally, if the Active Directory schema has not been extended or if Active Directory and Microsoft DNS are not being used, a server locator point can be published to WINS to provide a mechanism for a client to interact and automate client interactions.

Using Server Locator Points

The SLP directly queries the associated site's database for the requested information. The client queries are small, and the SLP caches the requested information locally.

Configuration Manager 2007 clients can utilize the SLP during client installation or site assignment.

The SLP returns the available assigned site's site code for the assigned site for the Configuration Manager client.

Planning Server Locator Points

A server locator point should be installed in the Configuration Manager hierarchy if any of the following conditions are true:

- ◆ Logon scripts are used to initiate client installation.
- ◆ The Active Directory Schema has not been extended.
- Sites do not publish their site information to Active Directory.
- Configuration Manager clients will be automatically assigned to sites.

Considerations

A typical Configuration Manager 2007 hierarchy includes only one server locator point. SLPs are typically installed at the central site of your Configuration Manager hierarchy. Installation requires minimal planning since the SLP is supported only on primary sites. In cases where your environment requires multiple SLPs, you need to either specify the SLP at installation (using CAPINST. EXE only) or configure your sites to publish their SLP information to AD.

Locating Server Locator Point via AD

When your sites are configured to publish the SLP location to Active Directory, clients will be able to query all available SLPs until site assignment is attained. SLPs are contacted in the order of the SLP list retrieved from AD.

Locating Server Locator Point via WINS

When there are no published SLPs in Active Directory, Configuration Manager clients will fall back to WINS to resolve an SLP. The SLP will need to be manually registered in WINS. You can specify only a single SLP in a WINS database. The configuration of WINS replication and what clients access the WINS infrastructure will influence how you register the SLP in WINS. In cases where there are multiple, separate WINS databases that do not replicate, you can specify whichever SLP is relevant to the clients that utilize that separate WINS database. When you have a WINS topology that replicates its database, you'll be able to register only one SLP. The SLP is

registered with a name of SMS_SLP with the associated IP address of the server hosting the SLP. The client will query the WINS database for the SMS_SLP entry and access the IP address returned. Take the following steps to create a static SLP entry in WINS:

- 1. Open a command prompt.
- 2. Type netsh, and press Enter.
- **3.** Type wins, and press Enter.
- **4.** Type **server**, and press Enter.
- **5.** Type the appropriate add name command. For example:

add name Name=SMS_SLP endchar=1A rectype=0 ip={static IP of your SLP}

Software Requirements

Configuration Manager 2007 server locator points require the following:

- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- ◆ IIS 6.0 or higher is required.
- ◆ Local SQL Server access to the SMS database or a replica of the SMS database is required.

Implementing the Server Locator Point Role

Take the following steps to implement the server locator point role on a server:

- **1.** Open the Configuration Manager 2007 console.
- **2.** Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.
- **3.** Right-click the primary site server name, and select New Roles.
- 4. In the New Site Role Wizard, click Next.
- 5. On the System Role Selection page (Figure 4.41), under Available Roles, select the Server Locator Point box, and click Next.
- **6.** Review the Summary Details page, and then click Next and Close.
- 7. Review the slpmsi.log file on the primary site server logs directory for "Product: SMS Server Locator Point – Configuration completed successfully."

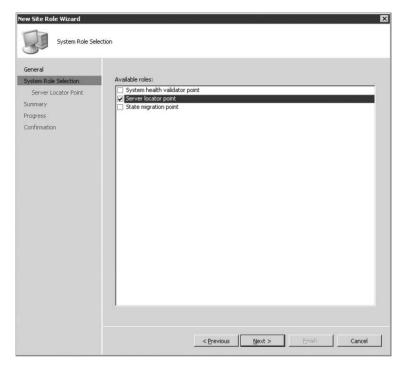
Troubleshooting a Configuration Manager 2007 Server Locator Point

This role assists the clients in finding and assigning to a Configuration Manager site. To ensure proper configuration of a healthy SLP, you should review the slpmsi.log file. This log is the MSI setup log for the server locator point.

SOFTWARE UPDATE POINT

This site system role is assigned to a computer running Microsoft Windows Server Update Services (WSUS). The function of the software update point is to provide software update metadata to clients that are using the Windows Update Agent (WUA) to scan for missing updates. The underlying component of the software update point is an installed WSUS 3.0 server with an additional Configuration Manager component. The additional component is called the WSUS Control Manager, which allows the Configuration Manager site server to control the behavior of the software update point.

FIGURE 4.41Selecting the server locator point role



The top-level software update point gets its metadata catalog from Microsoft Update and stores that catalog in its database. That database is also put into the Configuration Manager database via the sync process. For software updates scanning, Configuration Manager clients utilize the Windows Update Agent to connect with a software update point and get the specific metadata that are relevant for the client. The client is scanned for missing or installed updates and results from the scanning are stored in a WMI repository. The Configuration Manager client collects the results and passes them through the state message system, and those results are stored in the Configuration Manager database for every client and every update. Reports can then be generated from the scan data to produce accurate and detailed compliance reports.

Software updates are the topic of Chapter 6.

Software Requirements

Configuration Manager 2007 software update points require the following:

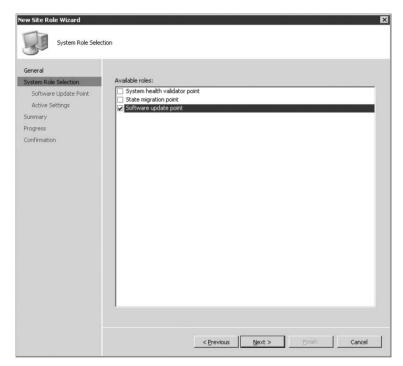
- All site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.
- IIS 6.0 or higher is required.
- WSUS 3.0 must be installed.

Implementing the Software Update Point Role

Take the following steps to implement the software update point role on a server:

- 1. Open the Configuration Manager 2007 console.
- **2.** Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.
- **3.** Right-click the primary site server name, and select New Roles.
- 4. In the New Site Role Wizard, click Next.
- **5.** On the System Role Selection page (Figure 4.42), under Available Roles, select Software Update Point, and click Next.

FIGURE 4.42 Selecting the software update point role



- **6.** If a proxy server is used, provide the appropriate settings as shown in Figure 4.43, and click Next.
- **7.** On the Active Settings tab (Figure 4.44), select Use This Server As The Active Software Update Point, assign the appropriate ports used in your enterprise, and click Next.
- **8.** On the Sync Source tab (Figure 4.45), leave Synchronize From Microsoft Update And Do Not Create WSUS Reporting Events selected, and click Next.
- **9.** On the Sync Schedule tab (Figure 4.46), select the Enable Synchronization On A Schedule box, and click Next.
- **10.** On the Classifications tab (Figure 4.47), select the appropriate classifications for your enterprise, and click Next.

FIGURE 4.43
Software Update
Point tab

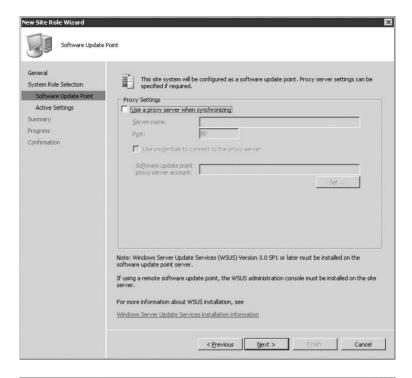


FIGURE 4.44
Active settings for software update point

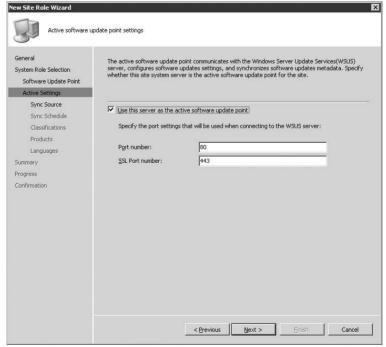


FIGURE 4.45
Sync Source tab

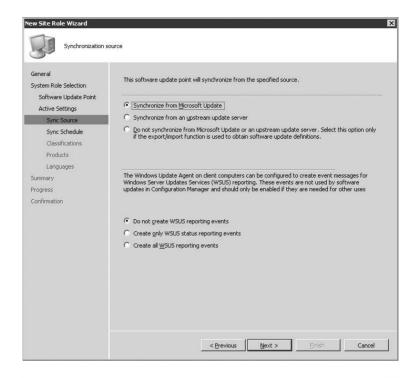
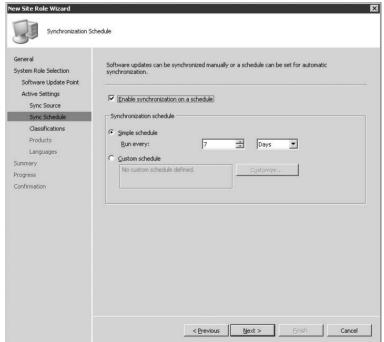
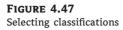
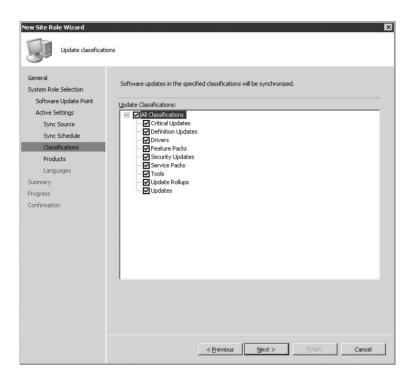


FIGURE 4.46
Sync Schedule tab







- **11.** On the Products tab (Figure 4.48), select the appropriate products to sync for your enterprise, and click Next.
- **12.** On the Languages tab (Figure 4.49), select the appropriate language(s) for your enterprise, and click Next.
- **13.** Review the Summary Details page, and click Next and then Close.
- **14.** Review the SUPSetup.log file on the primary site server logs directory for "Installation was successful."

Troubleshooting a Configuration Manager 2007 Software Update Point

Although you can almost classify the software update point role as essential, it still must be considered optional. This role's function is to interact with the WSUS 3.0 services to configure update settings, request synchronization from the upstream update server, and synchronize the WSUS database with the Configuration Manager 2007 database. The following logs provide insights into the proper configuration and health of a software update point:

supsetup. log This is the installation log for the software update point.

wsusctr1.log This logs activity to ensure connectivity is appropriate between Configuration Manager 2007 and WSUS.

wsyncmgr.log This log maintains the records of which updates were synchronized between the Configuration Manager 2007 database and the WSUS database.

FIGURE 4.48
Selecting products

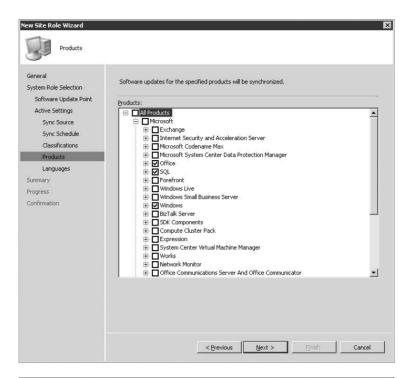
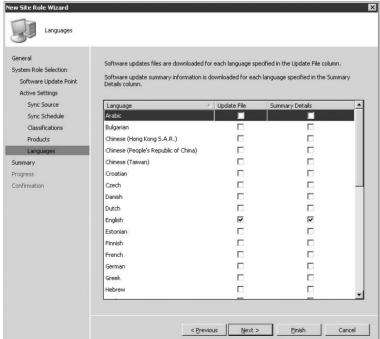


FIGURE 4.49
Language selection



STATE MIGRATION POINT

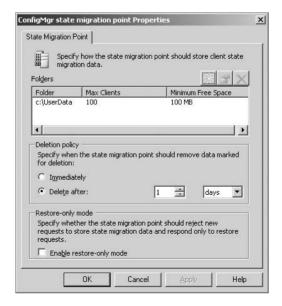
Think of the state migration point role as a reverse distribution point. The state migration point is a Configuration Manager site role that provides a secure location to store user state information before an operating system deployment. You can store the user state on the state migration point while the operating system deployment proceeds and then restore the user state to the new computer from the state migration point. Each state migration point site server can be a member of only one Configuration Manager 2007 site. (Operating system deployment is the topic of Chapter 8.)

Retention Policy

When you configure the state migration point, you can specify how long to keep user state data that was stored on it. The length of time that you keep the data on the state migration point depends on two considerations: the effect that the stored data has on disk storage and whether you need to keep the data for a time against the possibility of needing to migrate it again.

There are two phases to state migration: capture and restore. During capture, the user state data is collected and saved to the state migration point. During restore, the data is located on the state migration point, written to the destination computer, and then released by the task sequence step Release State Store. When the data is released, the retention timer starts. If you chose to delete migrated data immediately when you configured the state migration point, the user state data is deleted as soon as it is released. If you configured the state migration point to keep the data for a certain period of time, the data will be deleted when that period of time elapses after the state data is released (see Figure 4.50). The longer you set the retention period, the more disk space you are likely to need.

FIGURE 4.50
Configuring state migration point properties



Selecting Drives

When you configure the state migration point, you need to specify the drive on the server that should be used to store user state migration data. You select a drive from a fixed list of drives.

However, the list of available drives shows all drive letters available, some of which may represent nonwritable drives, such as the CD drive, or a non-network share drive. Some drive letters might not be mapped to any drives on the computer. Before configuring the state migration point, make sure you understand which drives are available to use for storing user state migration data.

Software Requirements

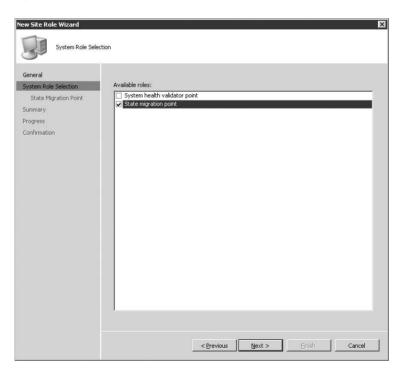
Configuration Manager 2007 state migration points require that all site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.

Implementing the State Migration Point Role

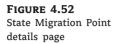
Take the following steps to implement the state migration point role on a server:

- **1.** Open the Configuration Manager 2007 console.
- **2.** Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.
- 3. Right-click the primary site server name, and select New Roles.
- 4. In the New Site Role Wizard, click Next.
- **5.** On the System Role Selection page (Figure 4.51), under Available Roles, select the State Migration Point box, and click Next.

FIGURE 4.51
The System Role
Selection page



6. On the State Migration Point details page (Figure 4.52), determine at least one folder to store user data, determine the Deletion Policy, and click Next.





7. Review the Summary Details page, and select Next and then Close.

Troubleshooting a Configuration Manager 2007 State Migration Point

This role is leveraged during the operating system deployment. In particular, it is used to store user data for migration back onto their machine that was just reimaged or replaced. The following logs will assist in properly setting up and troubleshooting the state migration point:

smssmpsetup.log This log documents the appropriate prerequisites and logs the initialization of the smp.msi file and installation completion.

smpmsi.log This log documents the installation setup progress of the smp.msi file.

SYSTEM HEALTH VALIDATOR POINT

The system health validator point is the site system role assigned to a computer running Network Policy Service. This role should be configured only if the NAP feature will be used.

The system health validator point is the Configuration Manager 2007 site system role that runs on Windows Server 2008 with the Network Policy Server role. When using NAP with Configuration Manager 2007, the system health validator point is needed to validate the statement of health from NAP-capable Configuration Manager clients to produce a client health state. This state may be compliant, noncompliant, or an error condition that prevented the health state from being determined.

The system health validator point validates a statement of health using a sequential series of checks. These include the following:

- ◆ Time validation when the statement of health was created
- ◆ Validation against the health state reference
- ◆ Compliance status and failures

The system health validator point never communicates directly with Configuration Manager 2007 site servers to validate client statements of health. When a Configuration Manager NAP policy is created or modified or inherited from a parent site, the site server writes a health state reference to Active Directory Domain Services. The system health validator point periodically retrieves the health state references for all Configuration Manager primary sites that are enabled for NAP.

Because Active Directory Domain Services is used to store the health state references, the Active Directory schema must be extended with the Configuration Manager 2007 extensions. The health state reference is published to a System Management container in Active Directory, which requires that Configuration Manager 2007 publishes site information to Active Directory Domain Services. When there is more than one Active Directory forest and your Configuration Manager site servers and system health validator points are not in the same forest, you must designate which forest and domain will store the health state references.

Software Requirements

Configuration Manager 2007 system health validator points require that all site servers must be members of a Windows 2000 or Windows 2003 Active Directory domain.

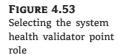
Implementing the System Health Validator Role

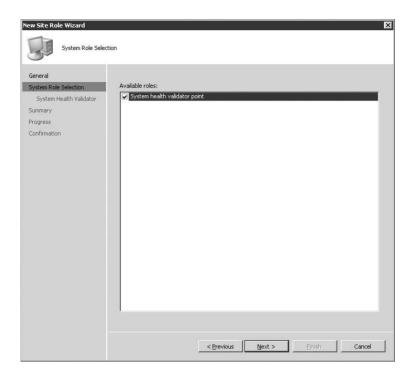
Take the following steps to implement the system health validator role on a server:

- **1.** Open the Configuration Manager 2007 console.
- **2.** Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.
- **3.** Right-click the primary site server name, and select New Roles.
- 4. In the New Site Role Wizard, click Next.
- 5. On the System Role Selection page (Figure 4.53), under Available Roles, select the System Health Validator Point box, and click Next.
- **6.** Click Next again on the following screen.
- 7. Review the Summary Details, and then click Next and Close.

Troubleshooting a Configuration Manager 2007 System Health Validator Point

Within the entire NAP scenario, this role allows the infrastructure to validate the statement of health from a NAP-capable Configuration Manager client. For troubleshooting, use the SMSSHVSetup.log file, which documents the prerequisite and installation progress.





Installing and Configuring System Center Configuration Manager 2007 Service Pack 1

System Center Configuration Manager 2007 Service Pack 1 was introduced six months after Configuration Manager 2007 was released in November 2007 so that the Configuration Manager product group could quickly integrate further innovations into the currently shipping product. They were able to introduce these innovations, as well as the foundational plumbing that is leveraged in Configuration Manager 2007 Release 2 (R2), because of the product's stability. Configuration Manager 2007 Service Pack 1 introduces the following general features:

- Support for agent-managed Microsoft Windows Vista Service Pack 1
- ◆ Support for agent-managed Microsoft Windows Server 2008
- Support for System Center Configuration Manager 2007 SP1 server roles on Microsoft Windows Server 2008
- Out-of-band management with Intel Active Management Technology (AMT) devices
- Update to Asset Intelligence 1.5

Out-of-Band Management

Out-of-band management is primarily used when the operating system becomes unresponsive to in-band management software such as Configuration Manager 2007. Out-of-band management

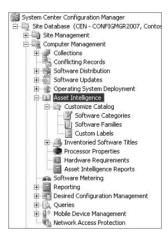
introduces the ability for Configuration Manager 2007 to communicate directly with Intel Active Management Technology (AMT) 3.x chip set or higher hardware. This allows Configuration Manager to enable hardware-based power management control and provide a vast array of remote diagnostic and recovery capabilities.

With its vPro chipset, Intel is the first hardware vendor to provide direct hardware interactions to leverage Windows Remote Management capabilities. These capabilities include remote boot control, forced PXE boots, remote network boots, and direct inspection of the hardware inventory and power state (although the machine's operating system may be powered down). These capabilities become very attractive when addressing geographically dispersed branch offices where there is little or no support staff to physically remediate workstations.

Asset Intelligence 1.5 Update

One of the larger parts of Configuration Manager 2007 Service Pack 1 is the update to Asset Intelligence. SP 1 introduces Asset Intelligence 1.5, which becomes its own node within the Configuration Manager 2007 console. Figure 4.54 shows this console node, and Figure 4.55 shows the Asset Intelligence home page.

FIGURE 4.54
The Asset Intelligence node in the console



As discussed in Chapter 9, Asset Intelligence builds upon the native hardware and software inventories to cross-correlate hardware and software attributes. The first steps within the custom catalog are to place software into categories and then group software into families. The following are some standard software category examples:

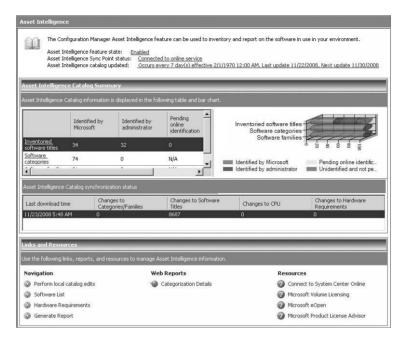
- Browsers
- Content management
- Finance and accounting
- ◆ Line of business

Products are then grouped into software families. These are some common examples of these:

- Communications
- Operating environment

- Productivity and viewers
- ♦ Security

FIGURE 4.55
The Asset Intelligence home page



The overall goal of the Asset Intelligence catalog is that software can be categorized and then placed into families so that enterprise reports can be generated from these attributes. Figure 4.56 shows a portion of the Asset Intelligence catalog reflecting a category and family.

FIGURE 4.56
Asset Intelligence sample products

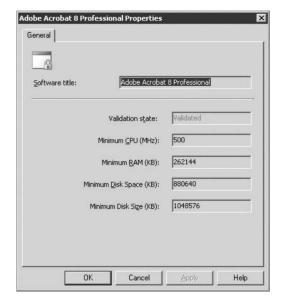
Microsoft Silverlight 1.0	Microsoft	1.0.20725	Browsers	Productivity and Viewers
Windows Internet Explorer 7	Microsoft	20061107.210147	Browsers	Productivity and Viewers
Adobe Flash Player 9 ActiveX	Adobe	9.0.45.0	Browsers	Productivity and Viewers
Windows Internet Explorer 7	Microsoft	20061107.210147	Browsers	Productivity and Viewers
Microsoft Internationalized Domain Names Mitigation	Microsoft		Development R	Application Development
Windows Presentation Foundation x64	Microsoft	3.0.6920.0	Development R	Application Development
Microsoft National Language Support Downlevel APIs	Microsoft		Development R	Application Development
MSXML 6.0 Parser Update (KB933579)	Microsoft	6.10.1200.0	Development T	Application Development
Windows Workflow Foundation	Microsoft	3.0.4203.2	Development T	Application Development
MSXML 6.0 Parser Update (KB933579)	Microsoft	6.10.1200.0	Development T	Application Development
Microsoft Visual C++ 2005 Redistributable	Microsoft	8.0.56336	Development T	Application Development
Microsoft Visual C++ 2005 Redistributable	Microsoft	8.0.50727.42	Development T	Application Development
Microsoft Visual Studio 2005 Premier Partner Edition	Microsoft	8.0.50727.42	Development T	Application Development

The next portion of Asset Intelligence provides administrators with insights into software license management. Software license data, Microsoft and non-Microsoft, can be imported into the catalog to enable more detailed reports and better license management in the enterprise. Improvements within the provided data relate to Client Access Licenses (CALs) for Windows products, such as Windows Server and Exchange Server, as well as the reports based on this data set.

The ultimate value of Asset Intelligence becomes most apparent within the Hardware Requirements node. This node is populated with software titles and their corresponding hardware requirements. Figure 4.57 shows an application's property sheet, which details the

minimum CPU, RAM, disk space, and disk size needed for a given application, in this case Adobe Acrobat 8.

FIGURE 4.57 Asset Intelligence: product hardware requirements



Only five shipping reports leverage the hardware requirements for a given application:

- ◆ Computers That Do Not Meet the Minimum System Requirements for Windows XP SP2
- Computers That Do Not Meet the Minimum System Requirements for Windows Vista
- ♦ Computers That Meet the Minimum System Requirements for Windows XP SP2
- Computers That Meet the Minimum System Requirements for Windows Vista
- Computers That Meet the Recommended System Requirements for Windows Vista

Beyond the built-in reports that ship with Configuration Manager 2007 SP1, Asset Intelligence definitely has the potential to be used in custom reports; that's a topic you'll want to explore based on the needs of your enterprise.

Software Requirements

The software requirements for Configuration Manager 2007 Service Pack 1 are identical to those for the release-to-manufacturing (RTM) version, with the additional support for Windows Server 2008 for Site Server Roles/Configuration Manager SP1 Agent as well as Windows Vista for the branch distribution point role/Configuration Manager 2007 SP1 Agent.

Implementing Configuration Manager 2007 Service Pack 1

To update your Configuration Manager 2007 implementation to Service Pack 1 (SP1), you must update your central site server as well as any distributed servers that may have roles running on

them. Once the central site server is upgraded, you can then take a top-down approach to ensure your entire hierarchy is running the same build of Configuration Manager. Take the following steps to implement Configuration Manager 2007 SP 1:

- Select Configuration Manager 2007 from the autorun screen, or start Setup. exe from the Configuration Manager installation media or from a copy of the installation media located on a network share or other storage media; this starts the Configuration Manager Setup Wizard.
- 2. Click Next on the Welcome page.
- **3.** On the Setup Options page, select the Upgrade Existing SMS 2003 or Configuration Manager installation option.
- On the Microsoft Software License Terms page, click I Accept These Terms, and then click Next.
- 5. On the Customer Experience Improvement Program page, choose a participation selection.
- 6. On the Updated Prerequisite Components page, select the appropriate option for obtaining the client prerequisite component files. Files can either be downloaded as part of the setup, or an alternate location where the client prerequisite component files have already been downloaded to can be used.
- 7. On the Updated Prerequisite Component Path page, specify the path to store client prerequisite component files downloaded during setup or the path to the alternate location where client prerequisite component files have previously been downloaded.
- **8.** On the Installation Summary page, review the summary details for the site installation before continuing. To make changes to any details, click Previous until you return to the relevant page in the wizard. After making any necessary changes, return to the Installation Summary page.
- 9. When the prerequisite checking has completed, review any messages in the results pane of the Installation Prerequisite Check page to verify that all prerequisites have been met for installation to continue. If no prerequisite errors are found, you can click Begin Install to begin the upgrade process. If prerequisite errors are found, you can review the ConfigMgrPrereq.log file located in the root of the system drive for more information about how to resolve any issues found. When all discovered prerequisite check failures have been resolved, return to the Prerequisite Check page, and rerun the setup prerequisites check.
- **10.** Review the installation steps on the Installation Status screen to verify the actions taken and their status as Configuration Manager is installing.

Troubleshooting the Configuration Manager 2007 Service Pack 1 Installation

The RTM version of System Center Configuration Manager 2007 is 4.00.5931.0000. Configuration Manager 2007 Service Pack 1 updates the version to 4.00.6221.1000. You can find this version code by performing the following steps:

- 1. Open the Configuration Manager console.
- **2.** Expand the Site Database node.

- 3. Highlight the Site Management node.
- **4.** Within the Details pane, review the version of the primary site server.

If the site version does not display version 4.00.6221.1000, review the ConfigMgrSetup.log file at the root of the OS drive of the primary site server. There should be an entry similar to Figure 4.58. (Note within this log that it documents the "Currently installed version.")

FIGURE 4.58
Service Pack 1 upgrade log

Review any potential errors and root cause of a service pack failure. Rerun Service Pack 1 if necessary.

Installing and Configuring System Center Configuration Manager 2007 Release 2 (R2)

In addition to the extended support and integration that System Center Configuration Manager 2007 SP1 introduced, it also provided the plumbing to support the new roles and features included within Configuration Manager 2007 R2, which was released September 2008. Some of these features are integration from tools previously available in SMS 2003, while other features are integration points to bridge other System Center products and technologies. The general features released in Configuration Manager 2007 R2 include the following:

- Integration of the Client Health Monitoring tool previously released for SMS 2003
- Integration of Microsoft Application Virtualization Management
- Integration of SQL Reporting Services
- Operating system deployment improvements
- Integration of Forefront Client Security

Client Status Reporting

Client health, historically, has always been a challenge. Distributing software or patches traditionally involved a statistical shell game. For example, let's say there were 100,000 clients in the enterprise that needed a particular patch. The way we used to describe it would be as follows: "There is a 98 percent success rate of all available clients for this particular patch." The reality of the software distribution would be that we targeted 100,000 clients, but only 80,000 clients were "available" to this given distribution. Thus, 20 percent of the clients out of the gate were deemed unavailable and were not reflected in the overall software distribution average.

In SMS 2003, Chris Sugdinis introduced the concept of *client health collections*. These collections would, in our example, take the targeted 100,000 clients and interrogate them about their health before attempting to distribute software to them. Client health extended to concept of query-based

collections and linking one collection's results to the next. Some examples of the questions are as follows:

- Is the client obsolete?
- ◆ Are the clients on a production subnet?
- ◆ Is the hardware scan older than 25 days old?
- ◆ Is there more than 50 MB free space on the logical disk?

In all there were 26 questions, at the end of which was a collection of clients deemed "all healthy clients." Within the tree of subcollections, clients that did not meet the criteria of a healthy client were dropped into an "unhealthy bucket," which then required remediation. This truly was the first insight into healthy or unhealthy clients that could be reported and remediated from an enterprise perspective.

Through the years, this concept was implemented in the product, leading incrementally to the features integrated into Configuration Manager 2007 R2. The data points you can now query for include clients that have not responded in a specified number of days, those not discovered in a specified number of days, and those that have not inventoried in a specified number of days. Configuration Manager 2007 can provide these insights, potentially through Internet-based client management and the like. Thus, if you are managing clients over the Internet, then hardware and software inventories should be flowing into the Configuration Manager 2007 site appropriately regardless of the connected state.

The client status reporting capabilities provide reports that lend insights into the potential client state. These reports include the following:

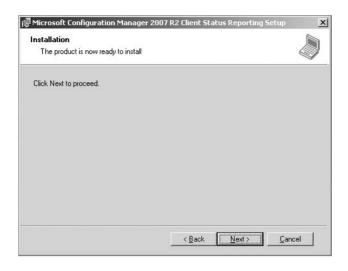
- Client Status Detail for a Specific Computer
- Client Status History (last 30 days)
- Client Status Summary
- Client Time to Request Policy
- Component Status History (last 30 days)
- Inactive Clients Detail

INSTALLING AND CONFIGURING CLIENT STATUS REPORTING

Client status reporting is an additional set of capabilities that you can install separately from Configuration Manager 2007 R2. This installation involves a few additional steps, which are counterintuitive if you're accustomed to the usual setup procedure:

- You can choose to install the feature from the R2 splash screen, or you can start by running clientstatusreporting.msi, which is found under the Client Status Reporting directory on your R2 media.
- **2.** On the client status reporting Welcome screen, click Next.
- 3. On the License Agreement screen, you'll need to accept the license; then click Next.
- This will present you with the Destination Folder dialog box. Change the path, if desired, and click Next.
- **5.** On the Installation page of the setup wizard, shown in Figure 4.59, click Next.

FIGURE 4.59
The Installation page of the Client Status Reporting Setup Wizard



6. The installation will not take very long, and you will be presented with the Setup Complete dialog box. Click Finish.

Administrators might expect all the client reporting capabilities to be available after running this installation routine, but a few additional items must be completed:

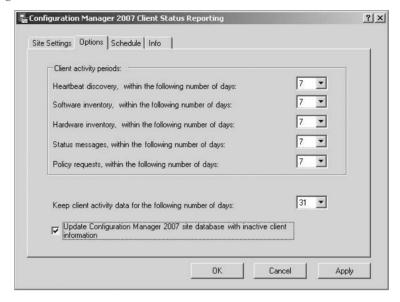
1. Navigate to Start ➤ All Programs ➤ Microsoft Configuration Manager 2007 R2 Client Status Reporting to run the Configuration Manager 2007 client status reporting configuration tool. The first configuration screen is the Site Settings tab, shown in Figure 4.60. This must be configured to connect to the site server and site server database as well as providing reporting service account credentials.

FIGURE 4.60
The Site Settings tab of the client status reporting configuration

ConfigMgr SQL server and in	nstance:	
	Example: server\instance	
ConfigMgr site database:		
Client status reporting service	account credentials	
C Use the local system acc	ount on this computer	
Use another account:		
Use another account: Account:		
	Example: domain\user	

2. You can set additional options via the Options tab shown in Figure 4.61, where you configure the different data points that compose the client health status. Since this data is retained in the Configuration Manager database, the client activity data retention policy is set up within this dialog box as well.

FIGURE 4.61
The Options tab of the client status reporting configuration



- **3.** On the Scheduling tab, shown in Figure 4.62, you can specify whether the client policy will request information from the management points and set a schedule for the request to run. This tab also allows you to schedule a ping of inactive clients. Client status reporting's client ping performs not only the standard ping commands but also checks the state of the Configuration Manager 2007 client service and BITS. The clients marked as inactive will be pinged following the schedule you specify here.
- **4.** The Info tab, shown in Figure 4.63, displays the version, the status, and details about the service.

Importing and Viewing the Client Status Reports

The final stage, which pulls together this entire solution, is to import and then run the custom reports that are delivered with this solution. The six reports listed earlier are valuable troubleshooting tools. Chapter 15 details the information each one contains, but briefly, they provide insights that will help you gauge the health of a Configuration Manager client. With these additional insights, an administrator can peel back the potential causes why the software updates or advertisement success rate is 96 percent instead of the expected 100 percent. These reports are delivered as a file named ClientStatusReports.mof, which is installed by default under the Program Files\Microsoft ConfigMgr Client Status\Reports directory. Take the following steps to import and then view these reports under the Reports node:

- Open the Configuration Manager 2007 R2 console, and traverse to Site Database ➤ Computer Management ➤ Reporting ➤ Reports.
- 2. Right-click Reports, and select Import Objects.

- 3. This starts the Import Object Wizard. Select Next.
- 4. On the MOF File Name tab, shown in Figure 4.64, type or browse to Program Files\Microsoft ConfigMgr Client Status\Reports, and select ClientStatusReports.mof. Click Next.
- 5. The Objects tab (Figure 4.65) lists the six new reports contained in ClientStatusReports.mof. Click Next, and click Next again on the (currently blank) Comments tab.

FIGURE 4.62
The Schedule tab of the client status reporting configuration

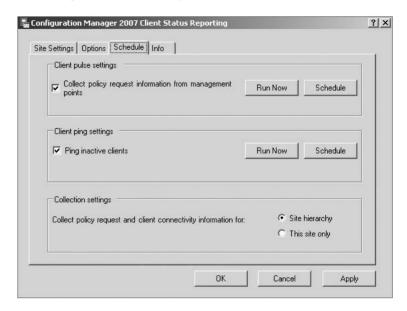


FIGURE 4.63
The Info tab of the client status reporting configuration

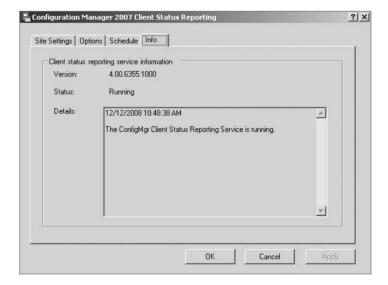


FIGURE 4.64
The MOF File Name tab of the Import
Object Wizard

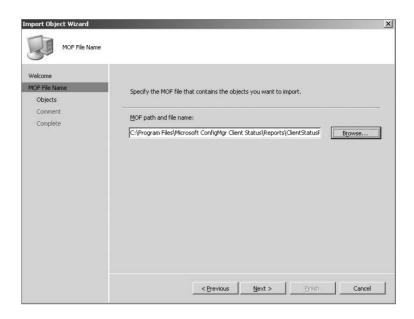
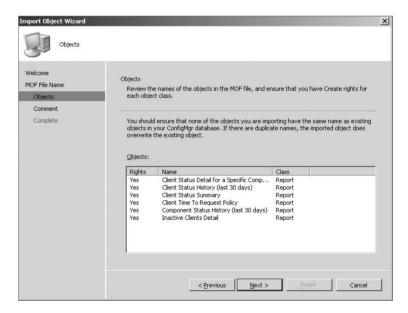
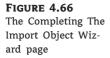
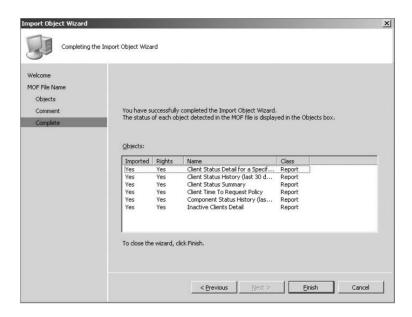


FIGURE 4.65
The Objects tab of the Import Object Wizard



- **6.** Finally, the Completing The Import Object Wizard page (Figure 4.66) appears, showing that you have successfully completed the Import Object Wizard. Click Finish.
- 7. Right-click the Reports node, and select Refresh.
- **8.** In the Reports Detail pane, sort by Category, and scroll down to the Client Status category.





Microsoft Application Virtualization Management

The infrastructure component of Microsoft Application Virtualization (App-V), formerly called SoftGrid, has been brought into Configuration Manager. There are a couple of distinct console changes as well as dependencies that must be performed to achieve software distribution of App-V packages via the Configuration Manager 2007 R2 infrastructure.

After installing Configuration Manager 2007 R2, you must enable your distribution points to allow virtual applications to stream from them. You can accomplish this by going to each distribution point's settings and selecting the Enable Virtual Application Streaming check box, as shown in Figure 4.67. This will allow the files as well as the virtual application sequences to stream to the App-V client via HTTP or HTTPS.

A dependency for client computers is that they need to have the Microsoft Application Virtualization desktop client licensed and installed. The package definition file (AppVirtMgmtClient.sms) is delivered with the installation of Configuration Manager 2007 R2. By default, it is located in the Tools/VirtualApp directory under the Configuration Manager installation directory, as shown in Figure 4.68. Although the package definition file is delivered with Configuration Manager 2007 R2, you must still obtain the App-V Client source from the appropriate channel such as the Microsoft Volume Licensing site.

Once the App-V client is distributed to those clients that you want to enable to run virtualized applications, you can then work on sequencing and ultimately distributing virtual applications to users and computers. Another console addition, shown in Figure 4.69, happens during the creation of a new package. As highlighted within Figure 4.69, you can natively import a virtual application package manifest XML file. This import wizard will import the sequenced application as well as reference the source location of the package when streaming them to the client.

SQL Reporting Services

One of the strategic directions of the System Center team is to standardize all the reporting capabilities within each of the System Center solutions to SQL Reporting Services (SRS). This allows a

single enterprise reporting engine to manage all reporting and takes advantage of the rich capabilities of SRS such as graphing, charting, scheduling, delivery, and exporting into different formats. In the current implementation of Configuration Manager 2007 R2, there are two web-based reporting solutions, which coexist side by side. All the original Configuration Manager 2007 reports have been ported to SRS for R2 with little or no additional features.

FIGURE 4.67Distribution point properties for App-V

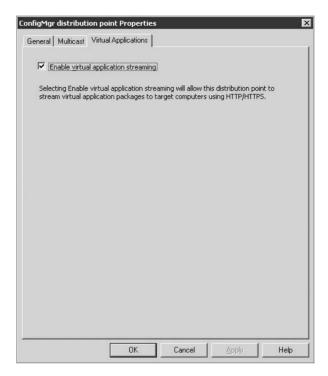


FIGURE 4.68
App-V package definition name and location

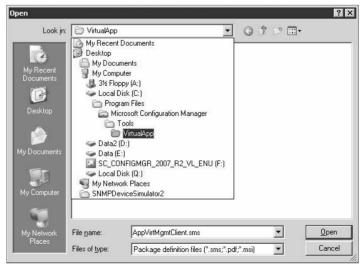
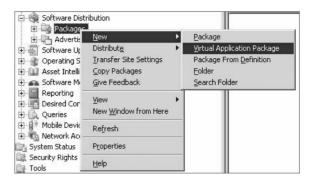


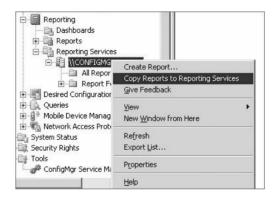
FIGURE 4.69 Importing a virtual application package



To take advantage of the SRS capabilities that Configuration Manager 2007 R2 now incorporates, you must take a few steps to configure this feature:

- 1. Install the SRS role within the SQL 2005 or SQL 2008 installation routine.
- Configure SRS with the Reporting Services Configuration Manager by selecting All Programs ➤ Microsoft SQL Server (2005 or 2008) ➤ Configuration Tools.
- 3. Add the new Configuration Manager reporting services point role under Site Systems.
- **4.** Traverse to the Reporting ➤ Reporting Services to configure the new server, which was installed in the previous step.
- Right-click the server, and select Copy Reports To Reporting Services, as shown in Figure 4.70.

FIGURE 4.70Selecting to copy reports to SRS



Operating System Deployment Improvements

Operating system deployment (OSD) is covered in depth in Chapter 8; here we'll preview its R2 enhancements. This feature has evolved since its inception within SMS 2003. With the addition of the Task Sequencer, which lets the admin rapidly produce production-ready builds from a single image, OSD in Configuration Manager 2007 already had most of the capabilities needed to build, provision, or migrate workstations and servers alike. Configuration Manager 2007 R2 introduces two needed capabilities to round out the build and provisioning scenarios.

MULTICAST AND THE GOLD IMAGE

First is the ability to target multiple machines to install their operating systems via multicast. The efficiencies of multicast drastically reduce the amount of bandwidth it would take to re-image tens or even hundreds of workstations simultaneously. Areas where you might have seen implementations are call centers, trader workstations (which are reset nightly), and kiosks.

Another great use of multicast is in the "unknown computer" scenario. Let's say, for instance, that you're undertaking a corporate-wide computer refresh, for which you're getting in a large number of machines daily or weekly. One option is that you can pay your computer vendor or reseller an additional fee to burn your gold image onto the incoming computers they are shipping to you. Another might be to have Configuration Manager 2007 R2 set up to service your build network or password-protect unknown computers to boot up onto your network and then leverage multicast to build your machines on-site.

Having your reseller ship your new computers with your gold image already on the new machines may seem like the path of least resistance at first, but think about a few nuances to that equation:

- How often do you have to update and deliver the gold image to your reseller?
- What's your build time once the computer is plugged into your build lab to customize it to your specific needs for a given machine?
- ◆ What does this added value from the reseller cost you?

Configuration Manager 2007 R2 allows you to retain your gold image on-site and deliver updates and customizations. Both the greater flexibility and the potential saving of additional costs may factor into your decision. Once the gold image is locked, it's irrelevant where that image lives; it could be stored internally or externally. The hidden power of Configuration Manager 2007 is the process that task sequencing brings to the table. You can leverage the work already done creating a baseline gold image for any system by customizing on top of it to address business user requests.

SOFTWARE UPDATES AND THE GOLD IMAGE

Note that an even simpler way of handling updates or patches to the gold image is to use software updates, covered in Chapter 6. The gold image is produced at a certain point in time and is applicable to that point in time. But subsequently, operating system or application patches may occur. With software updates, the admin can leverage work already done (creating the gold image) in combination with work that is being done (software updates management) to converge those efforts. Thus, when the image is deployed, all the current versions are applied at build time rather than having to build out an entirely separate process for each work item.

THE MICROSOFT DEPLOYMENT TOOLKIT

The other part of the OSD equation that has been revised is the Microsoft Deployment Toolkit 2008 (formerly the Business Desktop Deployment Solution Accelerator). As the original name suggests, it's a solution accelerator, allowing for a transparent set of processes, tools, and scripts to automate desktops and servers alike. Although the build process can be drastically different, such as building a domain controller or web server, most of the process has been automated from end to end within the Task Sequencer.

The Bottom Line

System Center Configuration Manager 2007 is built upon the collective learning of Systems Management Server that Microsoft has built on over the past 14 years. The foundational concepts have not varied drastically since SMS 1.0. These attributes are site types, site relationships, and various site roles.

Identify the different types of Configuration Manager 2007 sites. When discussing the Configuration Manager 2007 site types, they fall into three general types. Each one of these site types has strengths and weaknesses depending on the business scenario that is being addressed. When architecting a Configuration Manager solution, leverage all the available features within these types.

Master It List and describe the attributes of the three different types of Configuration Manager site types.

Define Configuration Manager 2007 site relationships. When multiple Configuration Manager 2007 sites exist within an organization, they have the ability to interact with one another. This interaction is known as site relationships. There are two distinct relationships between Configuration Manager sites.

Master It List and describe the two types of relationships of Configuration Manager sites.

Configure Configuration Manager 2007 site relationships. Once the architected solution has been drafted, the implementation of the Configuration Manager 2007 sites must be configured. To have visibility of all the enterprise assets, a site hierarchy must be established by leveraging site relationships.

Master It Create the central/primary site, and leverage a second server (physical or virtual) to install a secondary site server.

Enable and configure the essential Configuration Manager 2007 site system roles. When setting up a primary site server for a System Center Configuration Manager site, there are essential site system roles to enable immediately, while others are optional. The first and foremost is that there is at least one primary site server in the hierarchy; this is the first Configuration Manager 2007 server that is installed. Additional servers may or may not be added depending on the scale and availability needed.

There are essential site roles needed by Configuration Manager to perform the most basic of tasks such as client installation and inventories. Additionally, there are optional roles to install and configure in order to perform advanced functionalities. Not all site roles need to be installed and configured, and each role doesn't need its own server (a common misconception).

Master It Enable and configure the following site roles:

- Distribution point
- Management point
- Reporting point
- Server locator point

Chapter 5

Client Installation

For Configuration Manager to be effective, you will need to install the Configuration Manager client software on the client systems to be managed. In the previous chapters, we discussed all the planning and setup procedures for Configuration Manager. Carefully review the settings discussed in those chapters and make sure you have Configuration Manager ready for client installation.

This chapter covers the client software and how you can install the client, manage it, and ensure that it has been installed.

The client software can be installed either manually or automatically. Manual installation relies on someone physically running the setup program on each computer. Although manual installation is not the most efficient method, you may consider it when, for example, you have a remote location where you don't want to push the client software because of the limited bandwidth of a remote WAN connection.

In contrast, automatic installation methods deliver and install the software without human intervention. As you can probably imagine, this is the preferred method of deploying the client software. Once it is properly configured, you can use the Client Push method, which will allow the Configuration Manager Site server to install the client on any of the discovered systems within the site.

Many options are available to ensure that the client software is installed on each client within your organization, and this chapter covers the most important ones. Microsoft allows organizations to distribute the Configuration Manager client using any software distribution method already in place, including Group Policy Objects or logon scripts, or embedding the client within the operating system image.

Not every organization will need all of the functionality that is built in, so careful planning is a must in order to choose the options that best fit your environment.

In this chapter, you learn how to do the following:

- Configure Client Push Installation
- Configure Logon Script installation
- Manually install the client

Client Software Features

Each system that will be managed within the Configuration Manager infrastructure must have a client installed. The client software provides the interaction between the Configuration Manager Site systems and the client device. In essence, the client software is made up of multiple

programs, called *agents*, that can be enabled or disabled depending on the needs of the site. The agents that are present within the Configuration Manager client, shown in Figure 5.1, include the following:

FIGURE 5.1 Client agents



Hardware Inventory Client Agent Used to scan for and report hardware installed on the computer. The data that is collected is controlled by Managed Object Format (MOF) files, which you can manipulate on the site server. The MOF file defines the classes which will be added to WMI and thus reported back to the Site Server.

Software Inventory Client Agent Used to discover software installed on the computer. Inventory rules are used to determine the types of software files that are collected during a scan.

Advertised Programs Client Agent Used to determine when an advertised program is available for the computer or user. You can control the notification methods used when a program is ready for installation.

Computer Client Agent Used to configure settings for the client, including the account that is used to connect to the software distribution location, notification settings, and controlling BITS throttling.

Desired Configuration Management Client Agent Used to define the schedule that the system will scan for compliance based on the Desired Configuration Management rules.

Mobile Device Client Agent Used to configure the client on mobile devices.

Remote Tools Client Agent Used to control the Remote tools that are installed on a Windows 2000 system as well as the Remote Assistance settings for Windows XP and later systems.

Network Access Protection Client Agent Used to enable Network Access Protection compliance on systems as well as the schedule when scans will occur.

Software Metering Client Agent Used to run the rules that are configured to allow a system to record the software that is executing on the system.

Software Updates Client Agent Used to manage the software updates that are available from the WSUS server.

In the chapters that follow, we will be discussing each of the client agents in more detail. You should be aware of the following prerequisites for clients:

- ◆ Microsoft Background Intelligent Transfer Service (BITS) version 2.5
- ◆ Microsoft Windows Installer version 3.1.4000.2435 or later

- ◆ Microsoft Windows Update Agent version 7.0.6000.363 or later
- Microsoft WMI Redistributable Components version 5.2.3790.1830 or later
- Microsoft Remote Differential Compression (RDC)

Using Client Push Installation

Client push is the most popular method of client installation. When configured correctly, pushing the client to the systems becomes an extremely efficient and effective way to deploy the client. Once the client push is configured, this method will ensure that any new clients within the site get the client automatically.

Before you can enable Client Push Installation, there are some configuration settings that need to be reviewed, planned, and configured, or you will not be able to use this method. Specifically, you need to configure boundaries, create a Client Push Installation account, configure the discovery methods, and configure the client push settings. Then you can run the discovery process and, finally, enable client push. This section discusses each of the configuration items in detail.

Configuring Boundaries

Boundaries are a major component of Configuration Manager, and you need to give their configuration considerable thought and planning. They are critical not only for client assignment, but also for how the client handles software distributions. To oversimplify, boundaries are no more than IP address ranges that define the computers that are part of a Configuration Manager site. You have four ways of defining these IP address boundaries:

- IP Range
- ◆ IP Subnet
- Active Directory Site Name
- IPv6 Prefix

Using any of these options alone or in conjunction with one another, you can define the IP addresses that make up well-connected subnets and slower, less reliable subnets. Boundaries define how your site is configured. A site is a collection of clients based on boundaries defined by IP subnets, Active Directory Site names, or both.

Expanding Site Settings on the Configuration Manager console, you will see the Boundaries node. By default, its detail pane will be empty. To configure the boundaries for a site, right-click the Boundaries node and select New Boundary, shown in Figure 5.2. The New Boundary dialog will appear, giving you the opportunity to identify the IP address range. Figure 5.3 shows the options for identifying the site address ranges.

If you have already defined Active Directory sites that correspond to your site boundaries, you can take advantage of having one location to make changes to your boundaries. Once a site is defined in Active Directory, you can add it to the Boundary properties by changing the boundary Type to Active Directory Site, as shown in Figure 5.4; then, any changes that you make in Active Directory will be reflected in your site boundaries as well. Use the Browse button in this dialog to select an Active Directory site to use as a Configuration Manager Site boundary.

Creating the Client Push Installation Account

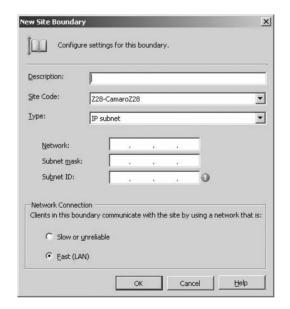
With the ever-increasing need for security measures, most administrators limit what the local end user has the ability to do on his or her workstation. A domain account can be created that has

the appropriate rights to install the client software on workstations that have been locked down. When the client software is pushed to a computer, an attempt is made to install the software using the user's credentials. If the user does not have the proper security rights to install software, the Client Push Installation account is used instead so that the client software can successfully install.

FIGURE 5.2
Creating a boundary



FIGURE 5.3
Boundary address options

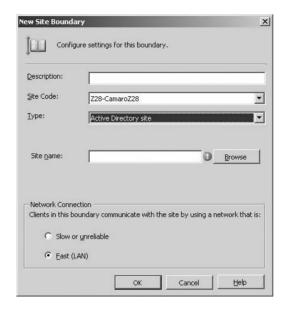


When you create the account, make sure you add it to the group within your Active Directory structure that has the proper security rights on each machine within the site. If the local account doesn't have local administrative rights, then it will use this account. Some Configuration Manager administrators put this account in the Domain Admin group because it is a simple way to ensure that they have enough rights on each client, but doing so is not necessary. The account only needs administrative rights on each client.

Once the account is created, you can open the Client Installation Methods node in the console, right-click the Client Installation Push Method and select Properties. Here you can select the Accounts tab and enter the account or accounts that will be used to install the client. Configuration Manager will attempt to install the client using the first name in the list. If authentication fails, it

will then try each account until it is successful. If it still fails after each of these accounts, then it will try the site server's computer account.

FIGURE 5.4The New Site Boundary Dialog box



Configuring Discovery Methods

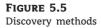
Discovery is the process by which Configuration Manager finds objects on your network that will be managed within your site. For client installation, discovery is required only when you are performing the Client Push Installation; all of the other client installation methods take advantage of other technologies. The Client Push Installation method requires the discovery process in order to identify the client systems to which the client software will be pushed.

When a system is discovered, a record is made of the discovered objects of the system, called the Discovery Data Record (DDR). The DDR contains information about the object discovered such as IP address, IP subnet, operating system, and other items (which depend on the type of device discovered). This information is just enough to identify the object. The DDR is then stored within the site database.

Computers are not the only items that can be discovered. Using the methods described here, you can discover users, groups, and network devices as well. Figure 5.5 shows the various discovery methods available within Configuration Manager.

Active Directory System Group Discovery To further identify computers within the site, a query utilizing Active Directory sites and services is sent to the nearest domain controller to find the system groups. Once the data has been returned to the database, the computers that are members of the system groups will have the system groups' detail reflected within the computer's attributes.

Active Directory Security Group Discovery Security groups that are created in Active Directory can be discovered using this discovery method. A query is sent to the nearest domain controller to locate security groups that meet the discovery criteria.





Active Directory System Discovery This discovery method is used to send a query to the nearest domain controller to find computers within the domain that meet the discovery criteria.

Active Directory User Discovery This discovery method sends a query to the nearest domain controller to find the user accounts that meet the discovery criteria.

Heartbeat Discovery This discovery method is enabled by default and used to notify the site server that the client system is still active. You can configure the interval that is used by Heartbeat Discovery to send the heartbeat to the site server. The default interval is 7 days, but can be configured to fit the environment requirements. You can disable the heartbeat, at which time it becomes the responsibility of the site server to determine that the system is up-to-date and active.

Network Discovery Network discovery is used to discover many different types of objects. Not only can you find computers that are on the network but any device that has an IP address can be discovered as well.

Each of the Active Directory discovery methods allows for only certain Organizational Units (OUs) to be discovered. This is helpful if you have a very diverse company within a single Active Directory domain. Each Active Directory discovery method can use custom LDAP querying to query machines that reside within a given location or Active Directory Organizational Unit.

When you first create your site, the only discovery method that is enabled is Heartbeat Discovery. You need to determine which of the other discovery methods you will need to use to find objects. Each organization has different objectives and therefore which discovery methods used within your organization will require some planning.

To configure any other discovery method, in the Configuration Manager Administrator console browse to Site Settings and click Discovery Methods to display the window you saw in Figure 5.5. Right-click on a discovery method, and choose Properties.

Selecting the check box in a discovery method's Properties window, as shown in Figure 5.6, will then enable that discovery process.

SCHEDULING OPTIONS

Each method also has a way of scheduling when the discovery will run. For the Active Directory discovery methods, the Scheduling tab resembles Figure 5.7 (in this case the Active Directory System Group). If you need to modify the schedule, click the Schedule button to display the Custom Schedule window shown in Figure 5.8. Here you can schedule on a weekly, monthly, or custom interval. If the discovery process needs to be done only on a manual basis, selecting the None radio button will prevent discovery from running automatically.

FIGURE 5.6
Enabling the discovery method



FIGURE 5.7 Scheduling tab for a discovery method



The Heartbeat and Network discovery methods have different configurations than the Active Directory methods and will need to be discussed separately.

The Heartbeat discovery method schedule is found on the General tab, as shown in Figure 5.9. Notice that you can set only a simple schedule for the Heartbeat; your options are much more limited than with the Active Directory methods.

You can create multiple schedules for the Network Discovery method, as shown in Figure 5.10. Configuring the options in the Custom Schedule dialog shown in Figure 5.11, you have a lot of

control over scheduling the Network discovery agent. Because of the time it could take for the network searches, you may want to configure a maximum runtime.

FIGURE 5.8
The Custom Schedule dialog

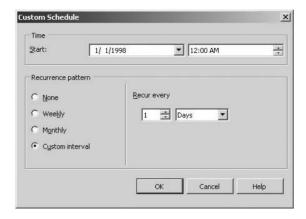


FIGURE 5.9
The Heartbeat Discovery
General tab



ACTIVE DIRECTORY SEARCH CRITERIA

Each of the Active Directory discovery methods allows you to configure the Active Directory locations that you will search, as well as the attributes that will be returned with the search. Because your Active Directory forest could potentially be rather large, with several thousands of objects, you may not want to start an LDAP request that has to parse through the entire directory tree. Instead, you may want to target the containers or organizational units that host the objects you want to discover.

Figure 5.12 shows the Active Directory Containers field that you use to define the locations where you want to search. When you click the New button, you are presented with the dialog

shown in Figure 5.13. This dialog allows you to enter the criteria for the LDAP query that is used for lookup. If you choose the Local Domain option, you are presented with a dialog to select the container within your Active Directory to search within. You can select any container or OU within the tree view. The Local Forest option is also available from this dialog, which allows you to start your query at the forest root, or any domain within the forest.

FIGURE 5.10The Network Discovery Schedule tab

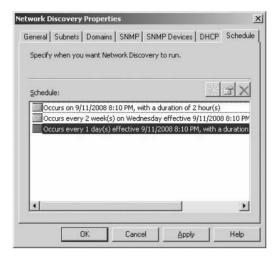
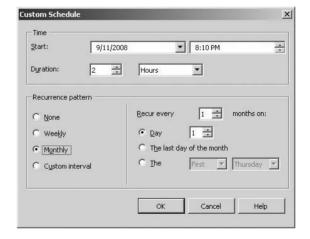


FIGURE 5.11
The Custom
Schedule
dialog for Network
Discovery



Once the start location for the query is chosen, the default behavior of the query is to search all of the child objects beneath the starting point. If you do not want to search through the child OUs, you can clear the check box labeled Recursive. This is a good way to limit the data returned from the query. With the Recursive check box selected, all of the containers and OUs within the object you selected will be searched.

You can use the Custom LDAP Or GC Query option to pinpoint the clients you want to discover. This option is bit more advanced, as it requires you to know LDAP Query Language, but it can be very useful when you want to pinpoint only certain clients within a large Active Directory. Because Global Catalogs can host information from all of the domains within the forest, it may be

more efficient to query the Global Catalog instead of sending the query to a Domain Controller within another domain.

LDAP QUERIES AND GLOBAL CATALOG QUERIES

LDAP queries start with LDAP:// and Global Catalog queries start with GC://. Otherwise the query statements will look identical.

FIGURE 5.12 Active Directory containers search criteria

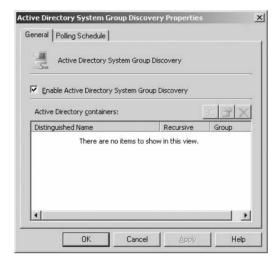


FIGURE 5.13
Selecting the containers to search



Real World Scenario

INSTALL THE CONFIGURATION MANAGER CLIENT ON EVERY MACHINE IN AN ACTIVE DIRECTORY OU

As the Configuration Manager administrator, you have been requested to install the client on a group of test machines within Production. What is your overall strategy?

- You work with your Active Directory team and they create an OU called ConfigMgr Test and place about 50 machines within that OU.
- 2. You open the Configuration Manager client and browse to Site Settings ➤ Discovery Method.
- 3. You then right-click on Active Directory System Discovery, choose Properties, and then click New to create a New Active Directory Container to search. You browse your Active Directory and find the OU called ConfigMgr Test.
- **4.** You specify your polling schedule and tell Configuration Manager to run Discovery as soon as possible.
- Now the systems are discovered with Configuration Manager and the client automatically installs on the machines.
- **6.** You verify that the clients are installed by looking at the logs on each client and then inform your manager.

Configuring Client Push Settings

Once the discovery methods have been configured, you will need to configure the client push settings to ensure that the client is installed correctly. In the Configuration Manager Administrator console, browse to Site Settings and then click Client Installation Methods. Now right-click Client Push Installation and choose Properties to display the General tab shown in Figure 5.14. Here, selecting the checkbox to Enable Client Push Installation to Assigned Resources means that whenever a computer is discovered within the Site boundaries, the client will automatically be installed.

After you enable client push, in the System Types area you can define which computer types will be included in the automatic installation by selecting any combination of workstations, servers, and domain controllers. You can also include Configuration Manager Site systems by selecting the checkbox at the bottom of the page. This allows you to update the client software on any site system that is discovered.

The Accounts tab, shown in Figure 5.15, allows you to specify the accounts to use to install the Configuration Manager client. Configuration Manager will try the accounts in order until it finds an account with administrative rights on the destination computer. It will always try using the sites server's computer account last if one or more accounts are listed, or only try site server's computer account if no accounts are listed.

In the Client tab of Client Push Installation Properties, shown in Figure 5.16, you control how that client is installed by entering Installation properties within the text box. Available installation properties range from the directory where the client is installed to the logging options that will

be used once installed. The properties that are included on this page will be used when the client push is used, whether by automated installation or initiated by an administrator from the console.

FIGURE 5.14 The General tab of Client Push Installation

Properties

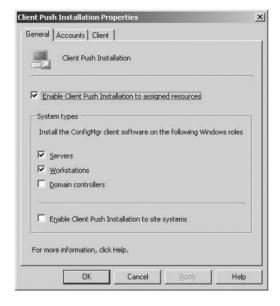


FIGURE 5.15
The Accounts tab of
Client Push Installation
Properties



The properties that can be entered in the text box are:

CCMAdmins This property allows you to configure which admin accounts are for the client. If more than one account, separate the accounts with a semicolon. Usage:

CCMAdmins=account1; account2; ...

FIGURE 5.16
The Client tab of
Client Push Installation Properties



CCMAllowSilentReboot After the installation is complete, if a reboot is required, this property will cause the machine to reboot without saving any user changes. Only needs to be specified if the silent reboot is to be used. A value of 1 forces the reboot if required. Usage:

CCMAllowSilentReboot=1

CCMDebugLogging Enables or disables debug logging. A value of 1 enables logging; a value of 0 disables logging. Usage:

CCMDebugLogging=0 | 1

CCMEnableLogging Turns logging on or off. If this property is not included, then logging is disabled. Usage:

CCMEnableLogging=True

CCMInstallDir This is the directory where the client software will be installed. Usage:

CCMInstallDir=installationfolder

CCMLogLeve1 Used to control the amount of logging activity. A value of 0 is verbose logging. A level of 1 logs all Information, Warning, and Error conditions. A level of 2 logs Warning and Error conditions. A value of 3 logs all Error conditions only. When included, you must also use CCMEnableLogging. Usage:

CCMLogLevel=0 | 1 | 2 | 3

CCMLogMaxHistory Controls the total number of previous log files within the Logs directory. When included, you must also use CCMEnableLogging. Usage:

CCMLogMaxHistory=NumberOfLogFilesToKeep

CCMLoxMaxSize Controls the maximum log file size. When included, you must also use CCMEnableLogging. Usage:

CCMLogMaxSize=LogSizeBytes

DisableCacheOpt When this property is included in the text box, it disables the cache configuration setting within the Systems Management properties in Control Panel. Users will not be able to manipulate the settings — only Administrators will be allowed to. Usage:

DisableCacheOpt=True

DisableSiteOpt When this property is included in the text box, it disables the Site Code configuration setting within the Systems Management properties in Control Panel. Users will not be able to manipulate the settings — only Administrators will be allowed to. Usage:

DisableSiteOpt=True

SMSCacheDir Controls the directory where the cache is created. Usage:

SMSCacheDir=directorypath

SMSCacheFlags Can be used to control how much space the cache can occupy and the location where the cache will be stored. When used in conjunction with the SMSCacheDir property, you have control over where the cache is stored. The flags are as follows:

SMSCacheFlags=PercentDiskSpace Used to control the size of the cache by allocating the total cache size as a percentage of the disk size. Cannot be used with PercentFreeDiskSpace.

SMSCacheFlags=PercentFreeDiskSpace Used to control the size of the cache file by allocating the total cache size as a percentage of the free space on the disk. Cannot be used with PercentDiskSpace.

SMSCacheFlags=MaxDrive Used to place the cache on the largest drive in the system. Cannot be used with MaxDriveSpace.

SMSCacheFlags=MaxDriveSpace Used to place the cache on the drive with the most free space. Cannot be used with MaxDrive.

SMSCacheFlags=NTFSOnly Used to control the placement of the cache drive on volumes formatted with NTFS.

SMSCacheFlags=Compress Used to compress the files within the cache.

SMSCacheFlags=FailIfNoSpace Used to stop installation of the client if there is not enough space on the drive for the cache.

SMSCacheSize Controls the amount of space in megabytes that the cache will consume. Usage:

SMSCacheSize=CacheSizeInMB

SMSConfigSource Controls where the configuration source files are stored. Usage:

```
SMSConfigSource=R | P | M | U
```

SMSHTTPPort Port used by the client to communicate with the management point if the port is different than 80. Usage:

SMSHTTPPort=8000

SMSNoWINSLookup Controls whether WINS lookup is allowed when the client is trying to locate the management point and the site code. When included, WINS lookup is disabled. Usage:

SMSNoWINSLookup=True

SMSSiteCode Controls the site code that is assigned to the client. Usage:

```
SMSSiteCode=Auto | SiteCode
```

For example, suppose you wanted to push the client to systems, using the following options:

- ◆ Install the cache in the \Cache directory on the largest drive.
- ◆ Allocate 10% of the drive for the cache.
- Enable verbose logging.
- ◆ Log files have a maximum size limit of 1GB.
- Five log files will be kept.
- ◆ The site code setting cannot be changed except by an administrator.
- ◆ The site code will be automatically discovered.

Your entry within the Property text box would look like this:

SMSSITECODE=AUTO SMSCACHEDIR=CACHE SMSCACHESIZE=10 SMSCACHEFLAGS=PERCENTDISKSPACE; MAXDRIVE SMSENABLELOGGING=TRUE CCMLOGLEVEL=0 CCMLOGMAXSIZE=1024000 CCMLOGMAXHISTORY =5 DISABLESITEOPT

Performing an Attended Client Push

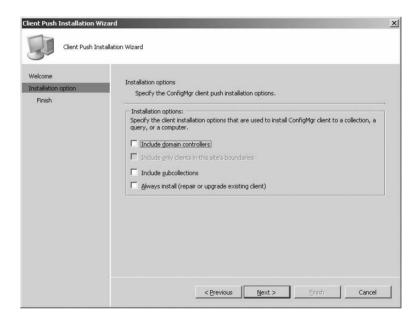
After discovery methods have been enabled and configured, and computer objects have been discovered, the client can be automatically installed on the discovered systems, or you can select the systems to which the client installation will be pushed. As we discussed in the "Configuring Client Push Settings" section, on the Client Push Installation > General tab, the Enable Client

Push Installation To Assigned Resources checkbox controls the automatic deployment of the client software. If you select the checkbox, the client will be installed automatically whenever a system is discovered. Depending on your site's configuration, you may not want to perform an automatic installation. This, however, would be planned out prior with your team.

In order to manually push the Client install out from within the Configuration Manager Administrator console, the target client system(s) needs to be discovered so that they will appear within the console under a collection. Once a system is available, you can push the client to the individual system, or you can push the client to all of the systems within the collection. The simplest way to do this is with the Client Push Installation Wizard. To initiate the wizard, right-click on the discovered system or collection and choose Install Client. This will open the Client Push Installation Wizard.

Although the properties and the installation account cannot be modified from the wizard, as Figure 5.17 shows, you can change some of the Client Push Installation options on an individual basis.

FIGURE 5.17Client Push Installation Wizard settings



From this page you can also choose to install the client on any system, whether it has been discovered as part of the site or not. Clearing the Include Only Clients Assigned To This Site checkbox will allow you to install the client on any system regardless of site assignment. You can also force the installation of the client, even if another client is already installed, by selecting Always Install (Repair Or Upgrade Existing Client).

To use client push to install to a collection, you can specify to install the client on all systems within a collection and any subcollections of that collection by right-clicking on the collection, and choosing install client. Selecting Include Subcollections will force the installation of the client on all of the systems in that collection and the clients in any subcollection within that collection.

Before you can push the client from the console, you will need to make sure the client is included within a collection. After locating the computer account within a collection, you can

push the client to the computer by specifying the options you want to use. To install the client on a Domain Controller, follow these steps:

- 1. Open the console.
- **2.** Navigate to Computer Management ➤ Collections ➤ All Systems.
- 3. Right-click All Systems and select Update Collection Membership.
- **4.** Wait a few moments while the command is sent to the site server and the database is queried.
- Refresh the All Systems collection and verify that your system is included in the details pane.
- 6. Right-click the system you want to install the client and select Install Client.
- 7. On the Welcome page click Next.
- **8.** Select the Include Domain Controllers option and click Next.
- 9. Review the settings and click Finish.

Other Automatic Installation Methods

Client Push Installation is not the only automatic method of installing the client. You can use other software distribution methods that are already in place within your organization. Using an existing software distribution product can ease the transition to Configuration Manager by distributing the client to the workstations, and then once Configuration Manager is in place, the existing software distribution product can be decommissioned.

Group Policy is another software distribution method that you may want to consider. You can start distributing the client software by using Group Policy, and then once Configuration Manager is in place, replace the Group Policy distribution with Configuration Manager's Client Push Installation. That way, all of the systems that should start working with Configuration Manager immediately will already have the client installed when you enable your site.

The other two options for automatic installation are using a logon script and creating a computer image. Each provides an efficient method of deploying the client, so it depends on how you need to deliver the client within your organization. Of course the imaging process works well for new systems that are being rolled out, and the logon script works well with existing systems. Evaluate your needs and configure the options accordingly.

Logon Script Installation

Logon scripts have been used by companies for many years to apply settings to users and their systems. They have become a popular method of setting configuration options because the logon script is directly tied to the user's account. No matter which computer the user logs on to, their settings follow them. While most logon scripts are simple commands that map drives and configure some basic settings, there are some pretty elaborate logon scripts that control the entire user environment based upon the user's group membership, departmental settings, and so forth.

To enhance a logon script so that it can be used to install the client is as simple as including the command line that defines the installation options and parameters. The parameters that you can use are the same as those detailed within the "Configuring Client Push Settings" section earlier in this chapter. The ccmsetup.exe command line allows you to define settings that control where

the installation files are located, the management point that will be used as the installation source, and the account the service will run under.

/source The /source switch is used to identify the location of the client.msi installer file. You can specify the switch multiple times to provide additional source file locations to provide for redundancy. Usage:

ccmsetup.exe /source:folderpath.

/MP The /MP switch is used to specify the management point that will be used as a source location. As with the /source switch, you can specify multiple management points by including the switch multiple times. Usage:

ccmsetup.exe /MP:Server

/UserOnly The **/UserOnly** switch is used to specify that the logged in user's account is the service account for the installation of the client. For this switch to work, the user account will need to have rights to install software; otherwise the installation will fail. Usage:

ccmsetup /UserOnly

/Service The /Service switch is used to install the client software using the security context of the local system account. For this to work, Active Directory has to be in use within your network and the computer's Active Directory account must have access to the installation directory where the client installation files are stored. Usage:

ccmsetup /Service

As an example, suppose you wanted an installation with the following options:

- Management point CHI-MP1 as the installation source.
- Run in the computer's security context.
- ◆ Install the cache in the \CCM\Cache directory on the drive with the most free space.
- ◆ Allocate 20% of the available free space on the drive for the cache.
- Enable verbose logging.
- ◆ Log files have a maximum size limit of 100 MB.
- Five log files will be kept.
- ◆ The site code setting cannot be changed except by an administrator.
- The site code will be automatically discovered.

The command line in your logon script would look like this:

ccmsetup /mp:CHI-MP1 /Service SMSSITECODE=AUTO SMSCACHEDIR=CCM\CACHE
SMSCACHESIZE=20 SMSCACHEFLAGS=PERCENTFREEDISKSPACE;MAXDRIVESPACE SMSENABLELOGGING=
TRUE CCMLOGLEVEL=0 CCMLOGMAXSIZE=100000 CCMLOGMAXHISTORY=5 DISABLESITEOPT

The client will install the first time the logon script runs after the command entry is included in the script. The initial configuration settings that are used with the installation command are used during the install. Most of them can be changed at a later time either manually or by running another script. After the command runs the first time, it will not run again. The system is checked to determine if the client is already installed, and if it is, the setup will stop without erroring out.

Imaging

The imaging method is a hybrid installation type. When creating a base image to be used for your organization, you will install the client software on the reference computer along with all of the other software that will be part of the image. As you are performing the installation, the key factor that you want to consider is that the client is not set to act as a member of any site. Setting the client so that it is site neutral allows you to deliver the image to a computer anywhere within your Configuration Manager implementation. When a client computer starts up the first time, it will determine which site it belongs to and will assign itself to the appropriate site. Note, if you are running in Native mode you will need to remove any client certificates.

When creating an image, the best method to use on the reference system is the manual installation. Manually installing the client will allow you to leave the site code field blank. You are essentially telling the client to go to sleep when you do so. The client will remain dormant until the next time the computer starts up. At that time, the client will query the closest domain controller to determine the site it belongs to. Once the client has determined its site, the site code will be configured and the client can start receiving policies from the management point. You will also need to stop the SMS Agent Host service by running NET STOP CCMEXEC prior to creating your image.

Manually Installing the Client

You can manually install the client by running CCMSetup.exe from the site server or from any management point. The file is located in the SMS\Client folder on the Site Servers and Management Points node within your Configuration Manager infrastructure.

There are some command line parameters to modify the behavior of the installation. A full list of installation parameters can be found by visiting http://technet.microsoft.com/en-us/library/bb680980.aspx. The following are the most commonly used parameters:

/mp: Z28MP01 Specifies the management point Z28MP01 to download the

client files from.

/logon Stops the installation if a previous version of the client is

already installed.

SMSSITECODE=AUTO Sets the sitecode to AUTO so the client will use the Active

Directory or Server locator point to determine the

Configuration Manager site.

Verifying Client Installation

As the installation is occurring, you can view the installation program running within Task Manager. If you have access to the system where the client is being installed, you can open Task Manager and you will see ccmsetup.exe running. As it completes, you will see ccmsetup.exe replaced by the Agent Host program CcmExec.exe, as shown in Figure 5.18.

You can also verify that the client has obtained the correct site code and is communicating with the management point. Open the Control Panel and you will find a new icon named Systems Management. When you double-click this icon, the properties appear. Clicking on the Advanced

tab, you should find the site code within the Currently Assigned To Site Code box, shown in Figure 5.19.

Within the Actions tab of the Systems Management properties, you should also find five actions listed by default, although other actions will appear in this list as the client agents are enabled. The default actions are Branch DP Maintenance Task, Discovery Data Collection Cycle, Machine Policy Retrieval & Evaluation Cycle, User Policy Retrieval & Evaluation Cycle and Windows Installer Source List Update Cycle. Each of these actions will be covered when we discuss the related components.

FIGURE 5.18
The Agent Host process running on the managed system

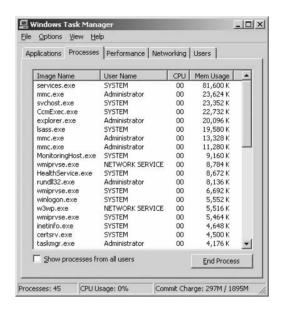
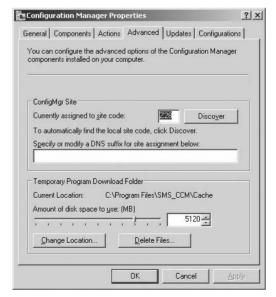


FIGURE 5.19
Verifying that the site code has been obtained



The Bottom Line

Configure Client Push Installation When configuring the Client Push Installation method, you need to make sure the required settings are in place. You must define boundaries, configure Active Directory extensions, configure the Client Push Installation properties, and run discovery methods to find the computer.

Master It You need to set up Configuration Manager to install the client software automatically on any client it discovers.

Configure Logon Script Installation When a logon script is used, the command line used to install the client needs to be included in the logon script, or a new logon script that uses the command should be created.

Master It The client needs to be installed on all of the systems within the domain. You want to roll out the client automatically while the end user is logging onto their systems, so you want to configure a logon script so that every machine will get the client when the machine is logged into the network.

Manually Install the Client Installing the client manually is also supported. An administrator needs to install the client on every machine where the client will be used.

Master It The client needs to be installed on all of the systems within the domain. You want to control the roll-out of the client, so you do not want to enable the ability for automatic installation, but you do want to use the push installation method so that you can control the installation from the console.

Chapter 6

Software Distribution

Software distribution has been among the most widely used features throughout the history of Configuration Manager, and it's also probably the most dangerous if not used properly. With the software distribution feature, you can send just about anything to a Configuration Manager client, from full software installations to a script that will add a shortcut to a user's desktop.

The danger with this feature is that there is no built-in functionality to create or validate what Configuration Manager distributes to its clients. If you haven't properly tested what you send out through Configuration Manager, it could lead to large-scale damage to your network in a relatively short time. The adage "garbage in, garbage out" definitely applies here.

Administrators will also need to pay attention to the choices that are available when starting a software deployment with this feature, because sending software out to the wrong computers or out at the wrong time could cause problems with even "safe" software.

Now this doesn't mean that this feature is a "loose cannon" and shouldn't be trusted. It just means that you should be familiar with software distribution and what it is capable of before using it. That is exactly what this chapter is all about.

In this chapter, you will learn how to do the following:

- Plan for software distribution
- Create and manage packages
- Create and manage programs
- Create and manage distribution points
- Create and manage collections
- Create and manage advertisements
- Monitor software deployments

What's New in Software Distribution

Taking feedback gathered from the previous versions of Configuration Manager and from intensive beta testing of System Center Configuration Manager 2007, Microsoft was able to greatly expand the features of software distribution with options that allow for a level of granularity in configuration that was not available in previous versions.

Here is a brief overview of those new options, which we will cover in more detail later in the chapter:

Branch Distribution Points (BDP) As described in Chapter 4, this is a new Configuration Manager server role designed for small branch offices that have minimal resources to manage or that may have poor network connectivity. BDPs function a lot like standard distribution points, but they provide greater control over network traffic by offering settings that can configure the scheduling and throttling of network traffic. They also allow for manual content provisioning and BITS enabling to further limit the use of network resources.

Maintenance Windows This is the most needed and welcome addition to software distribution and software updates. Administrators can now set a specific time frame when deployments are not allowed to run on a specific set of computers. This is an ideal option for organizations that have computers that must be left alone during business hours. Maintenance windows are set at the collection level and can be overridden in case there is an emergency.

Maximum Allowed Run Time program attribute This attribute existed in previous versions of SMS, but now it has more of a role in Configuration Manager because it is used in conjunction with maintenance windows. The Maximum Allowed Run Time program attribute you set is actually your educated estimate of how long it takes a program to run. If a program, such as a service pack to an operating system, takes 90 minutes to run and it is advertised to a computer in a collection with a maintenance window of only 60 minutes, then that program will not run. However, you can override maintenance windows if needed.

Improved rerun functionality for programs Administrators now have more control over when programs will rerun on clients with this enhanced functionality. The new options are more granular, and the number of options has also increased. Configuration Manager will also not allow an administrator to pick rerun options that are not compatible.

More control over program run and restarting options Administrators now have more control over program run and notifications settings, as well as being able to set bandwidth throttling, system restart countdown and notification, advertised program run countdowns, and notifications. Collections also now have specific restart and policy polling settings as well.

Custom client agent branding This was previously available only on software updates, but now Configuration Manager allows custom text specific to your organization to be displayed during software distribution and operating system deployment.

Better options for setting up new distribution points After making a new distribution point, you want to set it up with several of your organization's standard packages. In SMS 2003, you either had to go to each package one at a time and add the new distribution point, or you had to use a script. Configuration Manager now has a Copy Packages Wizard that allows you to copy multiple packages to the new distribution point.

Binary Delta replication Delta replication was available in previous versions of SMS but only at the file level. This became a problem during operating system deployment, because any changes in an image caused a new image file (which could be several gigabytes in size) to be copied to all updated distribution points, greatly increasing network traffic. With binary delta replication, only specific changes within a file are copied when distribution points are updated, which in turn reduces the amount of network bandwidth needed to update operating system images. This option can be used site to site, site to distribution point, or distribution point to branch distribution point.

Increased default cache size The default client program cache was increased a great deal in Configuration Manager, from 250 MB up to 5 GB. With the increasing size of software installs and with the frequency of security updates increasing all the time, this new cache size is more realistic in today's computing environment.

BITS-level resume now possible between distribution points Configuration Manager can leverage a new release of the Background Intelligent Transfer Service (BITS), which allows interrupted client downloads from BITS-enabled distribution points that pick up their download from where they left off from another distribution point and not just the distribution point the download started from.

Advertisements not replicated to secondary sites In SMS 2003, advertisement information is replicated to primary and secondary sites to support legacy clients. Configuration Manager no longer supports legacy clients, so this replication is no longer needed, which provides a boost in performance and a savings in network bandwidth.

Application Virtualization Management As described in Chapter 4, Configuration Manager 2007 R2 now supports running sequenced applications that were created using the Microsoft Application Virtualization (App-V) platform. This allows you to run virtual application packages on Configuration Manager clients without having to install the software application on the local computer. This will be explained in more detail later in this chapter in the "Virtual Application Packages" section.

Prerequisites for Software Distribution

Unlike some of the other features of Configuration Manager, software distribution does not have any specific prerequisites other than a working install of Configuration Manager. There are, however, some dependencies that exist internally to the software distribution feature.

Internal Dependencies

These are the internal dependences, all of which will be discussed in more detail later in the chapter:

Software Distribution component configuration The default setting of this component needs to be reviewed and configured if necessary for your environment.

Advertise Programs Client Agent This agent manages the software distribution feature's client connection and must be enabled before you can send software to clients.

Distribution Points Before you can send out software to a client, at least one distribution point must be enabled to host that software so clients can access it. Each site server has this server role enabled by default during a standard installation. However, the number and location of distribution points you need for any particular distribution will depend on the setup of your network environment.

Collections Collections are essential to software distribution because they organize the groups of clients that are the target of software deployments.

Package Access Accounts In most cases, the default access settings will work fine, but there may be cases where you need to set up special access to give clients the proper rights to access packages after they have been sent to distribution points.

Distribution Point Requirements

Table 6.1 shows Microsoft's prerequisites for the two kinds of distribution points, standard and branch. See "Using Distribution Points" later in the chapter for more details on each kind.

TABLE 6.1:	Microsoft's	Prerequisites	for Dis	stribution	Points
------------	-------------	---------------	---------	------------	---------------

PREREQUISITE	STANDARD DISTRIBUTION POINT	BRANCH DISTRIBUTION POINT
Operating system	Minimum server-class operating system for Configuration Manager	Minimum workstation- or server-class operating system for Configuration Manager
Have Configuration Manager client installed?	No	Yes
Computer must be on a domain?	Yes	Yes
IIS required?	Only if BITS is enabled	No, leverages BITS client
Require a standard distribution point on the same site?	No	Yes

Other requirements for the software distribution feature include the following:

Drive must be formatted as NTFS to use compressed source files There is an option to create a compressed version of the source files when you are creating a package. For this to work properly, the location for the source must be on an NTFS drive, because a FAT-formatted drive will not support it.

Disk space factors for site servers and distribution points Before making a package that will be sent to distribution points, you need to verify that there is enough disk space on at least one of the drives on the site server, on the distribution points, and on the all child sites that will host the package. Software distribution works fastest and most efficiently if you also have enough disk space to compress and decompress package files. Configuration Manager will start this process on the drive with the largest NTFS partition but will continue to the next largest drive if the first one fills up, and so on. If there is not enough space on any of the server's drives, the site server will have to wait for the removal of temporary package directories before it can continue to send out packages. If a site system runs out of disk space during the software distribution process, Configuration Manager will continue to complete package processing until it eventually times out. If you manually free enough space before the timeout period, Configuration Manager will continue on its own. Microsoft recommends the following guidelines for estimating free disk required for a package:

- If Configuration Manager is using the source files directly when sending out the package and the site server is also a distribution point, then the server will need space equal to the size of the package.
- If the package will be sent out to child sites, the site server will need additional disk space equal to 0.5 times the size of the package.

- If you store a compressed version of the source files, then the site server will need additional disk space about 1.5 times the space of the original source files.
- ◆ Each distribution point requires disk space equal to about 1.1 times the size of the uncompressed package source folder. This is necessary because a distribution point will need to store delta signatures recording changes as well as the original source files.
- ◆ If the site server performs a distribution point role, it will need free space approximately between 1 and 2.5 times the size of the original package source files.

Microsoft provides a good set of guidelines here, but as a safety margin, we recommend adding at least 25 percent to these numbers just so you will be covered.

Elements of Software Distribution

Before you can plan to use software distribution, you will need to know about the different elements that are part of that feature and what role they play in the software distribution process.

Software distribution uses what is called *packages* to deploy software to clients, while *programs* are what are defined in packages that tell the client what exactly to run when it gets there. *Advertisements* are what are sent to clients to let them know which programs of a package to run, when to run them, and which computers are going to run them. To get that all to work, other elements, such as the Advertised Programs Client Agent, also need to be configured.

The Advertised Programs Client Agent

The Advertised Programs Client Agent controls what advertised programs should run on the client or for a user logged on to the client. When a client finds an advertisement assigned to it, the Advertised Programs Client Agent is what will find and connect to the nearest available distribution point, either to download the package locally to run or to run it from the distribution point itself. If the program calls for a local file to be run, it will do that with the settings defined in the program. This agent also controls how often clients check for advertised programs and how they act when an advertisement is discovered to be available.

To use software distribution, you must enable the Advertised Programs Client Agent and then configure it to your specific needs. Keep in mind that these settings, like all Configuration Manager client settings, are for the entire Configuration Manager site and can't be configured differently for each Configuration Manager client on the same site.

To find the Advertised Programs Client Agent, go to the Configuration Manager console, and navigate to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ Site Name ➤ Client Agents. Its options are grouped into two tabs, General and Notification.

THE GENERAL TAB

Figure 6.1 shows the General tab of the Advertised Program Client Agent's Properties dialog box. The General tab has the following options:

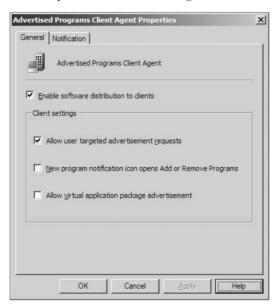
Enable Software Distribution To Clients Selecting this box enables software distribution for Configuration Manager clients. If this option is disabled, then other Configuration Manager features such as software updates and operating system deployment will not work either, because they use Software Distribution components to operate.

Allow User Targeted Advertisement Requests This setting allows users to be targets of a software deployment, no matter what client computer they are logged on to. If you clear this

box, the Configuration Manager client will not look for new user-targeted advertisements even if they are already available, but current ones will still run. To stop user-targeted advertisements altogether, you must disable the program being advertised, expire the advertisement, or delete the user-targeted advertisement. (Deleting an advertisement before it has expired isn't really recommended; it causes more problems than it solves.)

New Program Notification Icon Opens Add Or Remove Programs You can configure the New Program notification icon to show up in the client computer's taskbar. When this option is selected, it allows the icon to open Add or Remove Programs in Control Panel.

FIGURE 6.1
General tab



THE NOTIFICATION TAB

Figure 6.2 shows what the Notification tab for the Advertised Program Client Agent's Properties dialog box looks like. The options here control how advertised programs notify clients of deployment activity.

When New Advertised Programs Are Available This section configures how clients are notified when new programs are available; it has two options:

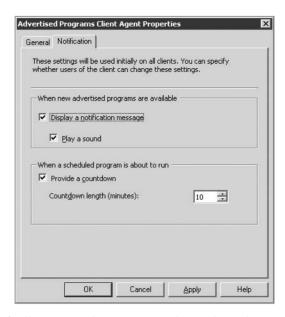
Display A Notification Message Select this option to display a visual notification message on the user's desktop.

Play A Sound This is pretty self-explanatory. When a new program is available, a sound will play.

When A Scheduled Program Is About To Run This section configures what happens when a scheduled program is about to run; it has only one option:

Provide A Countdown If you want your advertised programs to show a countdown before they run, then select this box, and set how long before a program runs that the countdown will begin.

FIGURE 6.2
Notification tab



Unless your organization specifically requires these options to be used, we don't recommend them. They may cause unnecessary panic and could potentially increase help desk calls.

Packages

Configuration Manager uses packages to send software to clients. When you think of packages, you might think of a software program that is installed on a Configuration Manager client, but a package might also consist of files that need to be copied to a client or a command to run files that are already present on the client computer. Packages will often contain the source files for whatever software you are sending to your clients. If this is the case, you will need to configure the package to specify the location of the source files and the distribution points that will host the package files for clients. See "Creating Packages" later in the chapter for more information and examples.

Programs

Programs are the part of a package that defines what a client is supposed to do with the package when it arrives for use at a Configuration Manager client. You can have a program do just about anything, including installing software, copying files to the client, running security software already on the client, or changing a client's configuration. Anything that you have an install or a script for, you can make a program to run it for you.

There should be at least one program per package that you are sending to clients, but you can have as many programs as you need. A common way to use programs is to have one for installing a piece of software with user interaction and another to install a program silently in the background with a standard configuration so it will not interrupt the user while they are working.

For a program to work properly, it must contain all references to install files and their command switches, if those are required. The program will also define what security rights the program will run under and what operating systems can run the program. See "Creating Programs" later in the chapter for more information and examples.

Distribution Points

Distribution points are site servers that store files for packages so they can be run by client computers. Think of a distribution point as a warehouse for storing packages and their files so clients can use those files when they are needed, either by downloading the files to run locally or by running them directly from the distribution point.

For a client to run an advertised program that is not stored locally, you have to make sure that a client has access to at least one distribution point so they can access the files of that program. With that in mind, it is recommended that you make available at least one distribution point for each Configuration Manager site in which the target collection has clients.

All site systems are set up as distribution points by default, but you can always remove that role and set it up on other servers as needed to take a load off a site system.

NETWORK BANDWIDTH CONSIDERATIONS

Clients that download packages from distribution points can greatly increase network traffic if you don't take the proper precautions. To spread out the load of a software distribution, you need to make sure that there are enough distribution points to handle the traffic of clients downloading programs. If needed, you can also put distribution points into groups so that client downloads can be distributed across the distribution point group instead of one single distribution point.

You can also designate a distribution point as *protected* by specifying which site boundaries a client must be located within before it can use the protected distribution point. Any clients that aren't in those boundaries will not be able to use packages on that distribution point. This will allow an administrator to isolate certain distribution points from unwanted network traffic.

Besides standard distribution points, you can use two other options for making package source files available to clients:

Distribution point on a server share A distribution point can also be set up on any server share that you specify. The advantage of this is that you can specify which drive packages will be copied to. This is the only site system role that you can assign to a share. You must keep in mind that Configuration Manager will not create a data discovery record (DDR) for a share, and it will not be able to monitor things such as space left on the share or whether the share's hosting server is offline. You can get around that by assigning the hosting server as a site system but not assigning any site roles to it. Also note that configuring both the share and the hosting server is not supported; it will cause both to become unreliable as distribution points.

Branch Distribution Points (BDP) This new site system role was designed for small branch offices with limited network bandwidth. They function pretty much like standard distribution points and are typically used when 10 or fewer clients are at a location. However, a BDP provides several advantages that help minimize network bandwidth by leveraging BITS when downloading packages. This technique also enables admins to control the transfer rates of packages, and it allows them to restart at a checkpoint if a package is interrupted during download. A BDP can also provide the On-Demand Package Distribution option, which allows a package to be sent to the BDP only after it has been requested by a client at that branch, so bandwidth isn't used if it isn't needed.

Since a BDP doesn't have the functionality of a secondary site, it can't function independently and requires connectivity to a BITS-enabled standard distribution point to get its content. BDPs can be set up on either a workstation or a server.

Advertisements

Once you have made a package and sent it to the proper distribution points, you will need to send the package to the appropriate client computers. You do this by advertising the program you want to make available to a collection of clients that you want to run the program.

An advertisement contains the following information:

- ◆ Which program is to run on the client.
- ♦ Which collection of computers, users, or user groups is to get the program.
- When the program will be available to clients, for how long, or whether the program will be mandatory. You can also set whether you want Wake On LAN to be enabled for the advertisement, as well as whether the program is important enough to ignore any maintenance windows that a collection might have.

Collections

Collections are vital to software distribution because they represent groups of resources such as computers, users, or user groups that you can organize into manageable units reflecting the kinds of resources in your environment and how you want to manage them.

When you set up an advertisement for a program to run on clients, it is a collection that is the target of that advertisement. Only the resources in that collection are assigned the program in the specified time frame of the advertisement.

Collection membership either can be by direct assignment or can be query-based. With direct membership, you will have to specifically define which resources belong to that collection and will have to manually update that collection as resources are added or deleted. Query-based membership is dynamic, so you do not have to manually manage the resources in the collection, and it is updated automatically on a specific schedule.

You can also use *subcollections* to manage resources, which allow you to associate one collection with another. Members of subcollections are not considered members of the containing collection, since collections can be a subcollection of multiple collections. Subcollections do not inherit the attributes of the parent collection. Each subcollection has its own identity and membership rules, which are completely separate from the parent collection. Most things you can do to a collection can also be done on its subcollections, and some can even be done at the same time, like both being the target of advertisement.

There are two types of subcollections:

Dependent subcollections These are created as new collections under an existing collection, which is dependent on the parent collection, as long as you don't link any other collections. When you delete a collection, all of the dependent subcollections are deleted as well.

Linked subcollections These are created when you link one collection with another collection that already exists. When you delete a collection, any linked subcollections are not deleted if they are an independent collection or a subcollection of another collection. This is true until all but one of the linking collections has been deleted, which then makes that subcollection dependent on the remaining one.

You can make subcollections under a subcollection to almost any depth, but that makes the collections more complicated and harder to manage, so we recommend not making too many levels of subcollections unless it is absolutely necessary.

Configuration Manager creates 16 default predefined collections when it is installed. They group resources in several common configurations and are listed in Table 6.2.

TABLE 6.2: Default Configuration Manager Collections

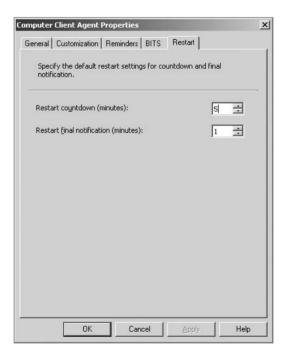
COLLECTION	DESCRIPTION
All Active Directory Security Groups	Security groups discovered through Active Directory security group discovery
All Desktops and Servers	All discovered desktop and server computers
All Systems	All computers and resources with IP addresses discovered by any means except AD user discovery
All Unknown Computers	Added with R2 to support unknown computer operating system deployment scenarios
All User Groups	All user groups discovered by AD user discovery
All Users	All users discovered through AD user discovery
All Windows 2000 Professional Systems	All computers using Windows 2000 Professional
All Windows 2000 Server Systems	All computers using Windows 2000 Server
All Windows Mobile Devices	All discovered Windows Mobile devices
All Windows Mobile Pocket PC 2003 Devices	All discovered Windows Mobile devices running Pocket PC 2003
All Windows Mobile Pocket PC 5.0 Devices	All discovered Windows Mobile devices running Pocket PC 5.0
All Windows Mobile Smartphone 2003 Devices	All discovered Windows Mobile devices running Smartphone 2003
All Windows Mobile Smartphone 5.0 Devices	All discovered Windows Mobile devices running Smartphone 5.0
All Windows Server 2003 Systems	All discovered computers running Windows Server 2003
All Windows Server Systems	All discovered computers running Windows 2000 or Windows Server 2003
All Windows Workstation or Professional Systems	All discovered computers running Windows 2000 Professional, XP Professional, Vista Business, Vista Enterprise, or Vista Ultimate
All Windows XP Systems	All discovered computers running Windows XP

Preparing for Software Distribution

Now that you have reviewed all the elements of software distribution, you should consider the following configuration options before you begin sending out software to your clients:

- Decide whether you want to show a notification message when an advertised program is available; this option is on the Advertised Programs Client Agent's Notification tab, as was shown earlier in the chapter in Figure 6.2.
- Decide whether you want a countdown to be displayed when an advertised program is about to run, and decide how long it will be. This is also on the Advertised Programs Client Agent's Notification tab.
- ◆ Decide what the restart countdown and notification period will be for clients when restarts are required after software installs. You can find this in the Computer Client Agent Properties dialog box, as shown in Figure 6.3.

FIGURE 6.3
Computer Client Agent
Properties dialog box's
Restart tab



- ◆ Decide the location where you will store packages on the site server. This option is part of the Software Distribution component. From the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database Server Name ➤ Site Management ➤ Site Name ➤ Site Settings ➤ Component Configuration. Figure 6.4 shows the General tab that opens.
- On the BITS tab of the Computer Client Agent Properties dialog box (Figure 6.5), decide on the bandwidth throttling and BITS settings for branch distribution points and clients.

FIGURE 6.4
Software Distribution Properties dialog box's General tab

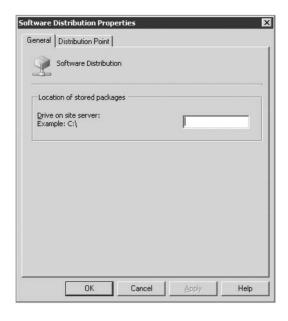
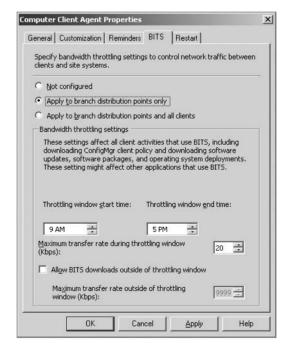


FIGURE 6.5 Computer Client Agent Properties dialog box's BITS tab



Determine whether any special rights are needed to run the program that is advertised. You set this on the program level of a package. If your users do not have administrative rights to their computers, you will have to configure a program to use other rights if the program requires it.



Real World Scenario

RUNNING SILENT

Your manager decides that from now on all distributions are to run completely invisibly to users, unless a reboot is needed. In that case, the user will get a 30-minute countdown so they will have plenty of time to save all their work and close all of their programs before the reboot takes place.

To make this happen, you will have to go through the various software distribution settings to disable all client notifications, while making sure that the client reboot settings are set to allow a countdown of 30 minutes before the reboot.

You start at the Advertised Program Agent by going to the Configuration Manager console and navigating to System Center Configuration Manager >> Site Database >> Site Management >> Site Name >> Client Agents to display the window shown in Figure 6.2 earlier in the chapter. On the General tab, make sure New Program Notification Icon Opens Add Or Remove Programs is not selected. On the Notification tab, deselect everything on the tab, and click OK.

From there, open the Computer Client Agent Properties dialog box, and go to the Restart tab. There you will find the restart countdown settings; input **30** in the Restart Countdown (Minutes) field, and click OK.

The Software Distribution Process

Assuming that you have already taken the steps laid out earlier in this chapter to plan, enable, and configure software distribution for your environment, you have to set up a deployment through software deployment. You'll perform some of these steps most of the time, but you might do others only if you start from scratch with a new package, programs, and so on. It all depends on what you are deploying in any given situation.

Gradually these steps will become second nature to you as you do them more often, especially now that Configuration Manager has more wizard-driven tasks to aid you along the way, unlike in SMS 2003, when you had to take a more "manual" approach to get the same job done.

The general steps are as follows:

- **1.** Choose or make a collection to be a target of the software deployment.
- 2. Create a package to distribute.
- **3.** Create a program for the package.
- **4.** Pick distribution points that will be needed.
- 5. Create an advertisement for distribution.

Now these steps are very basic, but they pretty much perform the core of just about any software distribution that you will come across. In some cases, these steps might have already been

done, such as if you are reusing a package that you have already used before, but that just makes the overall process that much faster. The following sections go through each general step in detail for a test application.

Creating Collections

Collections are an essential part of the software distribution process because they represent groups of resources that are the targets for software deployments. We introduced the basics of collections earlier in the chapter, so in this section you will learn how to create and manage collections. Collection membership either can be by direct assignment or can be query-based.

With direct membership, you must manually add the resources belonging to a collection and also manually update that collection as resources are added or deleted. Query-based membership is dynamic, so you do not have to manually manage the resources in the collection, and it is updated automatically on a specific schedule.

Direct membership in a collection should really be used only temporarily and sparingly. Collections are based on rules, so the more you use and rely on manual management in a system that is constantly changing, the less reliable they are.



SEND THESE COMPUTERS THIS PIECE OF SOFTWARE

As the Configuration Manager administrator, you will get various requests to deploy software to collections of computers on a regular basis. You will likely get multiple requests like this one: George T. Management sends a request to your boss to have the ACME Timewaster application installed for all the rest of the Big Management group. After asking some questions, you find out that the people in that group aren't in any one particular group in Active Directory that you can target, and they all have vastly different software and hardware. So, they have nothing in common that would let you easily make a collection based on a criterion to ensure that they all receive the advertisement.

Now, you could make a collection based on the entire Big Management group's user IDs, but you would hate to have the ACME Timewaster app installed on every computer that the Big Management group logs on to.

With all the reasonable options out of the question, your last resort is to ask for a list of computers that will need the essential ACME Timewaster program so you can make a collection with all those resources.

Three months later, you get your list of computers, make the collection, and deploy the software.

Now this might sound like an exaggeration, but any veteran SMS administrator has probably seen something similar at least once in their career. Collection based on direct membership is kind of a necessary evil, but it's recommended to use query-based collections if you can.

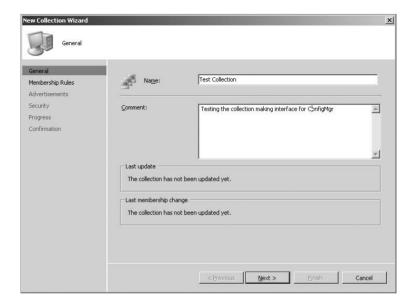
MAKING A COLLECTION WITH DIRECT MEMBERSHIP

Making a collection based on direct membership is relatively easy if you don't have too many resources to add at a time. If you end up with a large group of resources that you have to add, then you will have to resort to a script or something from the Configuration Manager Resource Kit.

To get started, you go to the Computer Management node in the Configuration Manager console. Inside that node is the Collections node. To make a new collection, right-click Collections, and click New Collection, which takes you to the New Collection Wizard.

The first thing you have to do is pick a name for your collection, and then you can optionally add a comment describing what the collection is for. After you have filled out that information, as shown in Figure 6.6, click Next to proceed.

FIGURE 6.6
Entering a name in the
New Collection Wizard's
General page



The Membership Rules page of the wizard, shown in Figure 6.7, is where you define your collection membership. The four boxes above the upper-right corner of the Membership Rules box show ways to enter the two methods of membership, the first one being for direct.

After you have read the text on the Welcome page, click Next. This brings you to the Search For Resources page, shown in Figure 6.8.

Figure 6.8 shows your first chance to input something into this wizard, and it gives you plenty of options. The top Resource Class gives you four options and, depending on what you select, gives you different options in the Attribute Name section of the page. The four resource classes you have to choose from are as follows:

- User Group Resource
- System Resource
- IP Network
- User Resource

Now, there are many options in the Attribute Name section once you select the resource class, but for this example, we will use System Resource, with the Name attribute as shown in Figure 6.9.

As you can see in Figure 6.9, after you select those two options, another check box, Exclude Resources Marked As Obsolete, becomes available. This is a great new option to this wizard in Configuration Manager, because it keeps you from wasting time with resources that aren't available anymore. (But for this example, it won't matter either way.)

FIGURE 6.7
Defining collection
membership in the New
Collection Wizard

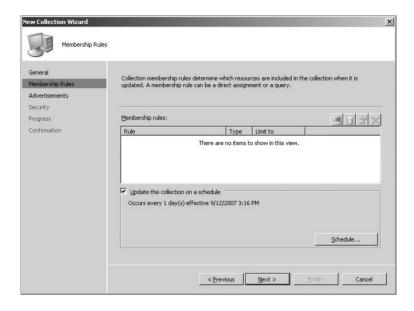
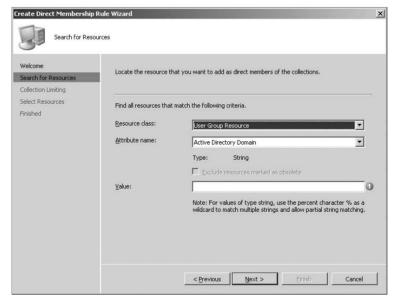


FIGURE 6.8
Searching for resources
in the Create Direct
Membership Rule
Wizard

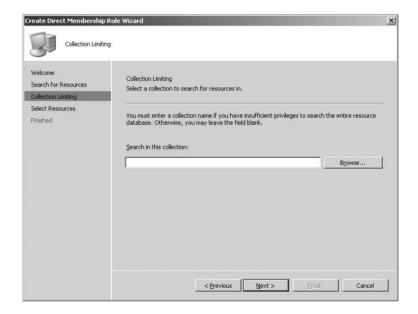


Now you come to what you have been waiting for. In the Value field, you have some options for cases where you have only part of the information you need. For example, say you know that all resources that you want to add start with the letter c. Since you can use wildcards in this field, by using the % symbol, you can just type c% to get a list all the resources matching those criteria that you can choose from. If you know that all of your resources have XP somewhere in their names, then you enter %XP%. In this example, there is a resource with XP in the name, so you type the wildcard value and click Next, which takes you to Figure 6.10.

FIGURE 6.9The Search For Resources page

Create Direct Membership	Rule Wizard	x
Search for Reso	ources	
Welcome Search for Resources Collection Limiting	Locate the resource th	nat you want to add as direct members of the collections.
Select Resources Finished	Find all resources that	match the following criteria.
1 maneu	Resource class:	System Resource
	Attribute name:	Name
		Type: String Exclude resources marked as obsolete
	<u>V</u> alue:	Note: For values of type string, use the percent character % as a wildcard to match multiple strings and allow partial string matching.
		< Previous Next > □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

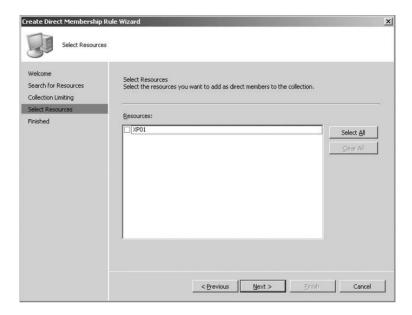
FIGURE 6.10
Limiting the collection
in the Create Direct
Membership Rule
Wizard



On the Collection Limiting page, shown in Figure 6.10, you can select an existing collection that you know your resource belongs to, if you need to narrow your search parameters. As it says in the text on that page, this might be your only option if you don't have the rights to search through all the Configuration Manager resources. That isn't the case in this example, so you can leave the field blank so you can search through all the resources.

Figure 6.11 shows you the list of resources that have matched the criteria you entered in the rest of the wizard, so you can either select the specific ones you want or just click Select All to add them all to the new collection. Click Select All for this example, and click Next.

FIGURE 6.11
Selecting resources



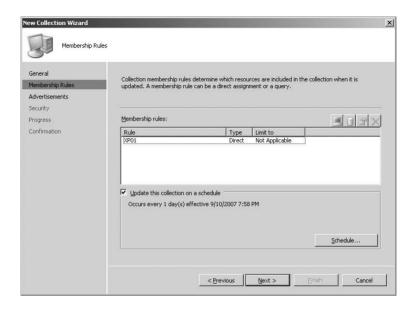
This takes you to the summary page shown in Figure 6.12, which shows you all the resources that you have selected and gives you a chance to go back and fix anything. For this example, just click Finish and continue.

FIGURE 6.12
Completing the Create
Direct Membership Rule
Wizard

Create Direct Membership	Rule Wizard	×
Finished		
Welcome Search for Resources Collection Limiting Select Resources Finished	Completing the Create Direct Membership Rule Wizard You have successfully completed the Create Direct Membership Rule Wizard. A new rule will be created for each resource you selected.	
	Resources:	¥.
	To create the new rules, click Finish.	
	< <u>Previous</u> <u>Next</u> > <u>Finish</u> Cancel	

As you can see in Figure 6.13, this takes you back to where you started, the New Collection Wizard, but now you see that the direct membership rule has been added.

FIGURE 6.13
Membership rule added



Below the Membership Rules box, you can see the check box for scheduling updates for this collection, and it has the default of once a day already added. For direct membership collections, that isn't really needed, because your membership rules are static and shouldn't change unless one of your resources becomes unavailable later.

Since you are finished with the membership rules for now in this example, go ahead and click Next to continue to the Advertisements page, as shown Figure 6.14.

This page shows any advertisements that are assigned to the collection you are making. It should of course be empty at this point, since you aren't really done making the collection yet. Let's click Next and move on to the Security page, shown in Figure 6.15.

Figure 6.15 shows the security rights already assigned to this collection and gives you the chance to modify them if necessary.

Class Security Rights This shows the user accounts and security permissions set for the collection object class. This applies to all collections in Configuration Manager. If you delete a user account here, it will change their rights for all collections.

Instance Security Rights This shows the user accounts that have rights on this specific collection.

Unless you know what you are doing, it's recommended that you leave the options here alone. Clicking Next here will start a progress dialog box, which might take a while depending on the size of the collection and the number of resources you have added.

Figure 6.16 shows you the Confirmation page, letting you know that your collection has been made with the criteria that you specified, and you can now see your test collection in the list of collections, as shown in Figure 6.17.

FIGURE 6.14
The New Collection Wizard's Advertisements
page

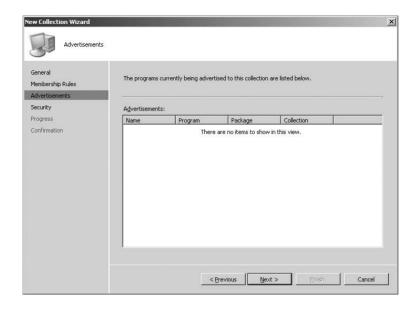
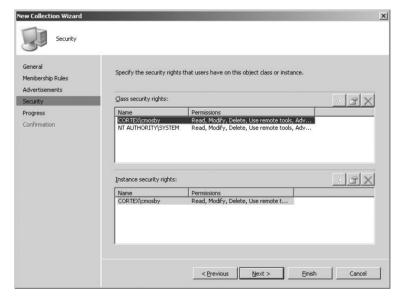


FIGURE 6.15The New Collection Wizard's Security page



MAKING A QUERY-BASED COLLECTION

Before we can show how to make a query-based collection, it will be useful to recap what exactly a *query* is. Wikipedia defines a query as "a precise request for information, typically keywords combined with Boolean operators and other modifiers in the field of information retrieval." Although this is a mouthful, it gives you a great idea of what a query is in Configuration Manager: a series of criteria that, together, are used to retrieve specific information from the Configuration Manager database.

FIGURE 6.16
The New Collection Wizard's Confirmation page

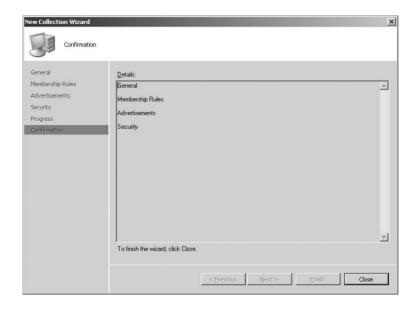
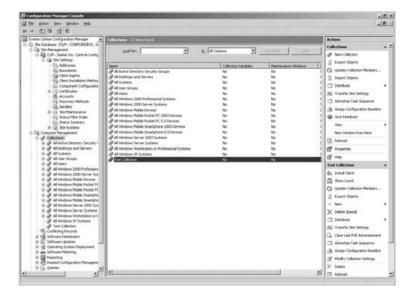


FIGURE 6.17
The new collection in the console tree



Many Configuration Manager features leverage information in queries that are pulled from the Configuration Manager database, but in the case of collections, queries are used to define what resources are included in collections.

To create a query, you need a minimum of two criteria: where to search and what to search for. For example, how many computers on your network have the Windows Vista operating system? Once you have made a query with the basic information that you need, you can always go back and add more criteria later. You can consider queries to be like quick mini-reports, instead of

making a more permanent report that goes on the reporting site. You can even export them into a .txt file or an Excel spreadsheet for use later.

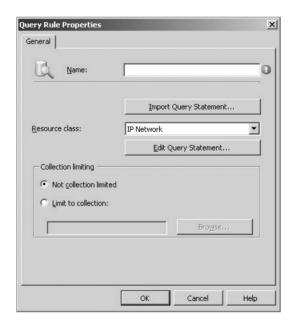
For the purposes of this chapter's exercise in creating a query-based collection, we created a query that we will use in our example. The query, called Virtual Machines, looks for resources that have *virtual machine* listed as their operating system.

To make a query-based collection, you start just as you did before. Go to the Computer Management node in the Configuration Manager console. Inside that node is the Collections node. To make a new collection, right-click Collections, and click New Collection. This opens the New Collection Wizard, as shown earlier in the chapter. After you name your collection (Virtual Machines in this case), click Next to move on to the page where you define your collection membership rules.

Here, instead of clicking the computer icon, as you did in the previous example, this time click the icon with the yellow cylinder (representing a database) to open the Query Rule Properties window shown in Figure 6.18.

FIGURE 6.18

Query Rule Properties
window



As you can see, you need to pick a name for your query rule and choose either Import Query Statement to use a query that has already been made or Edit Query Statement to make a query from scratch.

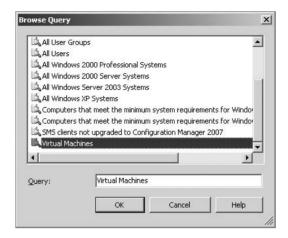
TAKE YOUR TIME AND GET IT RIGHT

We recommend that you make your query first under Queries node and get the bugs out of it and verify your results there. That way, you can fine-tune your results outside of a collection, which take a lot longer to refresh to show new results. Also, if you already had the package, program, and advertisement set up, software could be pushed out to a wrong set of users; it's always good practice to use queries first and then import them.

Even if you import a query that has already been made, you will still have to name your membership rule, because it won't take on the name of the query as it did in SMS 2.0.

When you click Import Query Statement, it will let you browse through all the queries that are in Configuration Manager so you can add what you need. For our example, we pick the Virtual Machines query created earlier, as shown in Figure 6.19.

FIGURE 6.19
Browse Query window



Once you have selected all that you need, click OK to return to the Membership Rules tab. Figure 6.20 shows you the Membership Rules tab after adding the query rule; you can adjust your update schedule. Because this collection is based on a query, it can be updated dynamically as resources that fit the criteria move in and out of Configuration Manager as they are discovered and retired. The default setting is for one day, starting at the time that you make the collection. Depending on what you are trying to show in that collection, that might be just fine. If you know that the resources in your collection are going to change rapidly and you want to be kept as up-to-date as possible, you can schedule updates to be more aggressive.

Just keep in mind that every time that a query-based collection updates, it is polling for updates to the collection from the Configuration Manager database directly. So, over time, creating a large number of collections with aggressive schedules could use up a lot of your site server resources.

From there, the New Collection Wizard continues just as it did for a direct membership, and you will eventually see it show up in your list of collections.

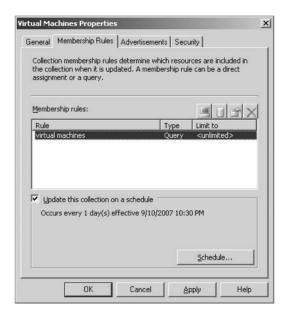
Creating Packages

Packages are what Configuration Manager uses to send software to clients and are the core of the whole software distribution system. Packages can be anything from a full-fledged software install like Microsoft Office 2007 to a script that changes the administrator password on workstations to just a shortcut that you want copied to your user's desktop. Packages will usually contain all the files necessary for your software deployment, such as files of the install DVD of Office 2007, but that isn't always the case, because a package can even be configured to run files that are already present on a workstation's file system.

You will probably have to create your packages from scratch, unless you are lucky enough to have a package definition file for the software you want to deploy provided by the software

vendor, where some of the package creation steps will be done for you. We will go over both methods in this chapter, but in both cases, you have to start by making your package in the Configuration Manager console.

Figure 6.20 Finished adding query rule



Before you do that, it is a good idea to create the source directory for any files that are going to be used in the package that you want to distribute.

KEEP IT ALL IN ONE PLACE

We consider it a best practice to put all the source files of all your packages in one folder and have each subfolder under that folder represent the source files of one package only. You can organize things further, for example by manufacturer, product, and so on, as you see fit. This will make your source files easy to find and back up when you need to do so.

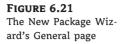
We also recommend that you keep the source files you use to develop your scripts and software files completely separate from your package source files so you won't get things mixed up.

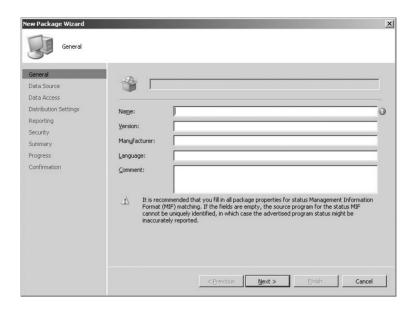
Remember, *everything* that is in the folder that you target as the source for your package files will be "bundled" up into your package. So if you have your final script and all your development files in the same place, they will *all* be sent to your distribution points when you send them.

CREATING A PACKAGE FROM SCRATCH

To make a new package from scratch, start from the Packages node of the Configuration Manager console by going to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Distribution.

From there you will see two nodes, Packages and Advertisements. Right-click Packages, select New, and select Package again. This starts the New Package Wizard, as shown in Figure 6.21.





In the opening page of the wizard in Figure 6.21, you can see what we mean by "from scratch"; all the fields on this page are completely blank, so you will have to fill them in. Also notice the red symbol with the white exclamation point showing that what is in that field is an "invalid name." Those warnings appear in all the wizards of Configuration Manager to help you make sure that what you are inputting is acceptable before you continue (of course, this doesn't compensate for bad spelling). Each field has certain limits on what you can enter, and some fields are required. The fields are defined as follows:

Name Enter the name of the package; this is a required field. This can be up to 50 characters.

Version Enter the version number of the package. This can be up to 32 characters.

Manufacturer Enter the manufacturer of the package. This can be up to 32 characters.

Language Enter the language of the package. This can be up to 32 characters.

Comment This is optional text; it can be up to 127 characters.

In Figure 6.22 you can see all the fields have been filled out, except for Comment, and all the warning signs are gone. The information for the software distribution test application (all the way back from the SMS 2.0 Resource Kit) has been entered, so you are now ready for the next step.

Figure 6.23 shows the Data Source page with its default settings. If your package didn't have any source files, then you could click Next and continue. In this case, we do have source files, so we select This Package Contains Source Files and continue.

In Figure 6.24 you see the options that become available after selecting the box. You will see the option to set the source directory for your package. When you click Set, another dialog box will open and give you additional options, as shown in Figure 6.25.

In this box, you browse to the location of your source files, either on the site server or on a location on the network, and click OK when you are finished.

FIGURE 6.22 New Package Wizard's General page filled by the package definition file

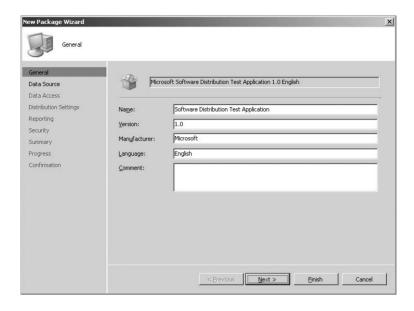
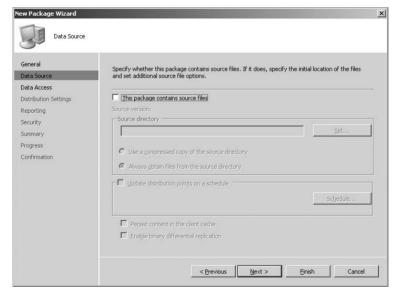


FIGURE 6.23
The New Package Wizard's Data Source page



In the Source Directory section of the Data Source page, you need to choose between these two options:

Use A Compressed Copy Of The Source Directory Using this option causes Configuration Manager to create a compressed version of the source files on the site server. That compressed version will be then decompressed and copied to the distribution points instead of pulling it from the original source folder when the distribution points are refreshed. This is a good option to use if the source files might be removed for some reason (for example, if they were housed

on a removable drive). Keep in mind that this option might use up extra system resources during the compression and decompression processes, depending on the files of the package and your site system configuration. This has been the case in previous versions of SMS, and it will more than likely be the case with Configuration Manager.

FIGURE 6.24The New Package Wizard's Data Source
Options page

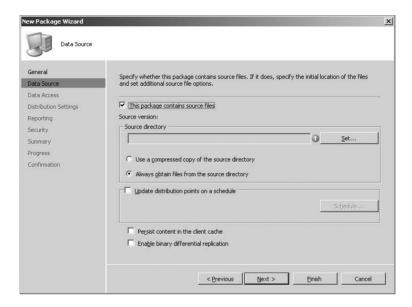
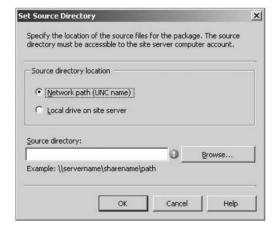


FIGURE 6.25The Set Source Directory dialog box



Always Obtain Files From The Source Directory With this option, every time that distribution points are refreshed, Configuration Manager will get the source files from the path that was specified in the Source Directory field. This is a good option to use if the source files will stay at that location or if the source files are going to be updated frequently.

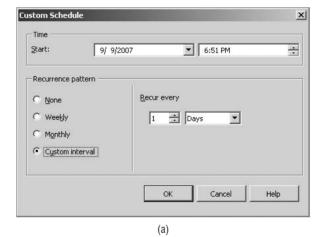
In the case of our test application, either of these options will work, but we will select Always Obtain Files From The Source Directory.

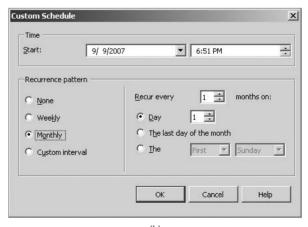
The next option, which is also shown in Figure 6.24, is Update Distribution Points On A Schedule. This option lets you set a schedule by which the source files of the package will be updated on distribution points. The default schedule is to update in one day, with the start time and date being the time that you checked the option box. Figure 6.26 shows you all the options for scheduling updates if you want to use it.

For this test application, you won't need to use that option. From there, there are two more options that are also shown in Figure 6.24.

Persist Content Client Cache This option will let your package stay in the cache in the client computer indefinitely even after it has been run. This could be useful for some packages that you use frequently, but we suggest using it sparingly because you could fill up the client cache with packages and cause a software deployment to fail later. The test application would be a good candidate for this option, but the purpose of it is to test the whole software distribution chain, so we won't use it in this example.

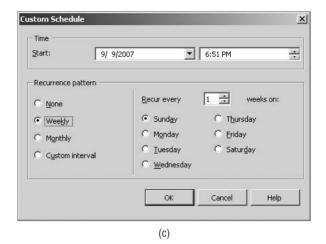
FIGURE 6.26 Custom schedules: (a) setting a custom interval, (b) setting a monthly interval, (c) setting a weekly interval, and (d) setting no scheduled updates





X

FIGURE 6.26 (continued)



(d)

Cancel

Help

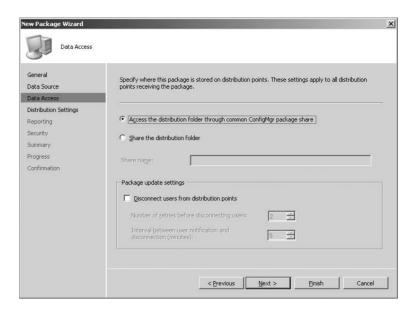
Enable Binary Differential Replication This selects whether binary delta comparison should be used on changed package source files. This enables the behavior that will allow Distribution Manager to transfer only the parts of a file that have changed instead of the entire thing. This feature was added to help with the large amount of traffic that came from sending updates with the traditional method to operating system distribution packages that could be several gigabytes in size. Using this feature on smaller packages won't do you much good, so we definitely won't use it in this example.

With that covered, you are finally ready to click Next. Figure 6.27 shows the Data Access page of the wizard.

These are the next batch of options:

Access Distribution Folder Through The Common Configuration Manager Package Share This option chooses to let users access the package through the common Configuration Manager package share (the standard SMSPKGx\$, with x being the drive letter the share is on).

FIGURE 6.27
The New Package Wizard's Data Access page



Share The Distribution Folder This option lets you pick a different share that has been created separately. If you select this option, you are required to input a share name in the field below. This name must be unique, even across package types, because duplicate names could corrupt the package. There are two options for the share name:

Network path (UNC name) In this case, all the files and subdirectories in that share will be deleted and re-created every time that the package is updated or refreshed.

Local drive on site server In this case, only the final directory in the path will be deleted and re-created each time it is updated or refreshed.

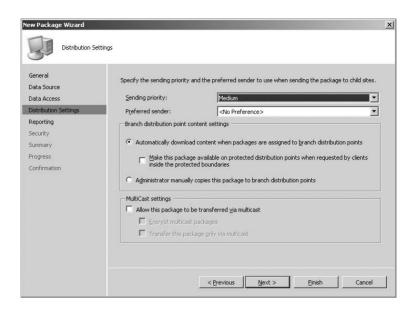
Disconnect Users From Distribution Points This box is selected by default, but it specifies the number of times that Configuration Manager will try to update the package source files before it disconnects users from the distribution point. If you decide to use this option, there are two settings:

Number Of Retries Before Disconnecting Users This sets the number of times that Configuration Manager will try to update a package before it will disconnect users who are connected to the distribution point. The default setting is 2, but you can set it anywhere from 0 to 99.

Interval Between User Notification And Disconnection (Minutes) This sets the number of minutes that Configuration Manager will wait before it notifies users before it disconnects them from a distribution point. The default is 5 minutes, but you can specify anything between 0 and 59.

The next page in the wizard is Distribution Settings, shown in Figure 6.28.

FIGURE 6.28The New Package Wizard's Distribution Settings page



Here are the options on this page:

Sending Priority This sets the priority of the package when it is sent to other sites. There are three options, High, Medium, and Low; Medium is the default. This option becomes useful if you have a package that needs to get out fast but there are other packages already being copied to distribution points. You can adjust the package priority to suit your needs in that situation.

Preferred Sender This sets the sender to be used while sending this package. The default is No Preference, which lets the package use whatever sender is available.

Automatically Download Content When Packages Are Assigned To Branch Distribution Points This is a default option and lets packages be automatically downloaded to all branch distribution points that are selected for the package. With this selected, you also get another option:

Make This Package Available On Protected Distribution Points When Requested By Clients Inside The Protected Boundaries This allows a package to be available for a new feature called *on-demand package distribution*, which allows a branch distribution point to download a package that it wasn't selected for, if a client that uses that branch distribution point requests to use a program from that package. This is available only for branch distribution points that have been made protected, and we will cover that later in the chapter.

Administrator Manually Copies This Package To Branch Distribution Points This is self-explanatory; the package is getting there, but Configuration Manager isn't going to be involved.

Clicking Next after setting the distribution options displays the Reporting page, which has the options shown in Figure 6.29.

FIGURE 6.29
The New Package Wizard's Reporting page

New Package Wizard		x
Reporting		
General Data Source Data Access	Specify how Management Information Format (MIF) files generated by clients apply to this package.	
Distribution Settings	© Use package properties for status MIF matching	
Reporting Security	C Use these fields for status MIF matching:	
Summary	MIF file name:	
Progress		
Confirmation	Name:	
	<u>V</u> ersion:	
	Publishers	
	< Previous Next > Einish Cancel	1

Use Package Properties For Status MIF Matching This is the default option, which means Configuration Manager will use the properties on the General tab of the package for status MIF matching. MIF files are covered in more detail in Chapter 10.

Use These Fields For Status MIF Matching With this option, Configuration Manager will use the values that you input into the available fields for status MIF matching. Unless this is filled out for you, we recommend sticking with the default option.

MIF File Name The name of the MIF file that contains the package status, which can be up to 50 characters

Name The name of the package, up to 50 characters

Version The version number of the package, up to 32 characters

Publisher The software publisher of the package, up to 32 characters

Figure 6.30 shows the Security page with the security rights already assigned to this package; on this page, you can modify them if necessary.

Class Security Rights This shows the user accounts and security permissions set for the package object class. This applies to all packages in Configuration Manager. If you delete a user account here, it will change the user's rights for all packages.

Instance Security Rights This shows the user accounts that have rights on this specific package.

After clicking Next to accept these settings, you are almost done, and the wizard displays its Summary page, as in Figure 6.31.

FIGURE 6.30 The New Package Wizard's Security page

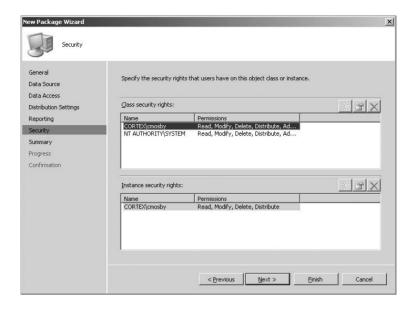
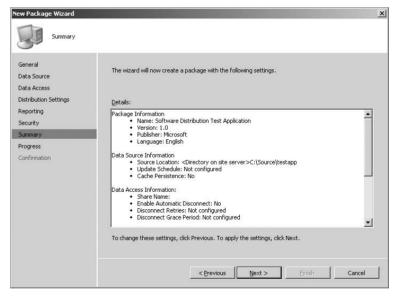


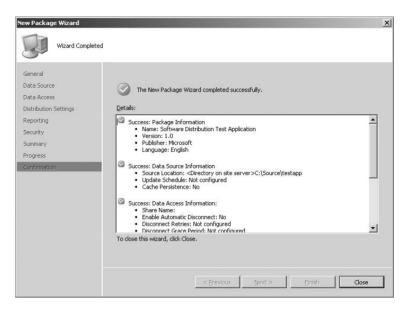
FIGURE 6.31
The New Package Wizard's Summary page



This page shows you all the options and settings that you have already chosen so you can review them and change them if necessary. If you are satisfied with what you see, click Next; otherwise, click Previous to fix what you need to fix.

When you click Next, you will see a progress page as the package is processed. This could be there for a while depending on the size of your package. When everything is done, you will see the Wizard Completed screen, as shown in Figure 6.32.

FIGURE 6.32
The New Package Wizard's Wizard Completed page



Success! You have made your first package from scratch.

You might have noticed that the wizard you just went through didn't ask you to select distribution points, as it did in SMS 2003 and previous versions. In Configuration Manager 2007, selecting distribution points for a package occurs later in the distribution process, and we will go through the steps later in the chapter.

CREATING A PACKAGE FROM A PACKAGE DEFINITION FILE

Now that you have made a package from scratch, let's take a look at making a package from a package definition file.

WHAT IS A PACKAGE DEFINITION FILE?

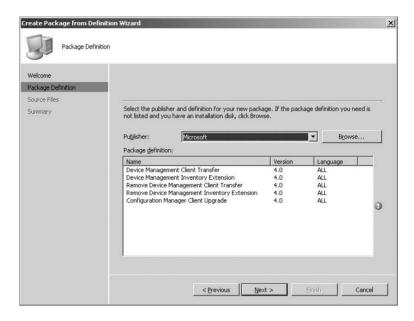
A package definition file is a script that is used to help automate creating packages in Configuration Manager. These files have all the package and program information needed to distribute a package, except for the location of the source files, which you will have to provide when you make the package.

Package definition files are often supplied with an application's install files by the software publisher. Configuration Manager also imports a selection of package definition files when it is installed and makes them available in the Create Package From Definition Wizard. You can get more package definition files and updates to existing ones on the Configuration Manager website.

To create a package from a definition file, you start just like you did before. Go to System Center Configuration Manager > Site Database > Computer Management > Software Distribution in the Configuration Manager console. When you go to the Package node this time, choose New > Package From Definition, and you will see the Create Package From Definition Wizard's Welcome page.

Once you have read the welcome message, click Next to proceed to the Package Definition page, shown in Figure 6.33.

FIGURE 6.33
Defining the package in the Create Package From Definition Wizard



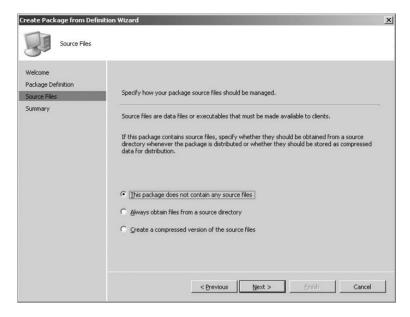
You can see that Microsoft has already provided some package definition files that you can use for various Configuration Manager tasks. If those aren't what you need, as in our case here, you can always browse the file system for the one you want, as shown in Figure 6.34.

FIGURE 6.34
Browsing for a package definition file



Notice in the Files Of Type field that you have three options for the type of your definition file: .pdf (not the Adobe kind), .sms, and .msi. In this case, pick the .sms file, and click Next twice to proceed to the Source Files page of the wizard, shown in Figure 6.35.

FIGURE 6.35
The Source Files page of the Create Package From Definition Wizard



As you can see, you have three options for the package source files, which are similar to what we discussed earlier in the chapter:

- The Package Does Not Contain Any Source Files
- Always Obtain Sources Files From A Source Directory
- Create Compressed Version Of The Source Files

For this example, we will choose the second option and click Next.

Figure 6.36 shows you the Source Directory page, which is similar to what you've already seen earlier in the chapter. We will pick Local Drive On Site Server for this example and enter the file's location.

You've completed the wizard settings, so clicking Next takes you to a Summary page (Figure 6.37), which allows you to review what you have selected and change anything if needed. Otherwise, you are done! Package definition files sure make setting up packages easier.

Creating Programs

Although a package has all the source files (or other information) that need to be sent to client computers, it is the program that actually tells the client what to do with the package files when it is time to run them. Each package should have at least one program that tells the clients what to do when the package arrives and should contain all references to install files, scripts, or command-line switches that are needed to run the program.

If you created your package from scratch, you will need to make the necessary programs for that package from scratch as well. If you used a package definition file to make your package, the necessary programs with all their information should already be created, though you may need to modify them to make them work in your environment.

FIGURE 6.36
The Source Directory
page of the Create Package From Definition
Wizard

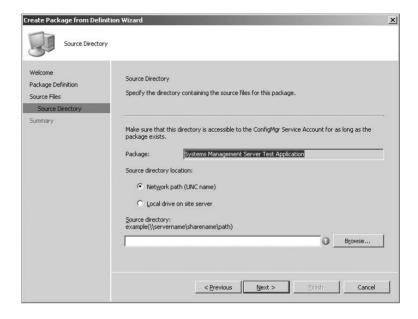
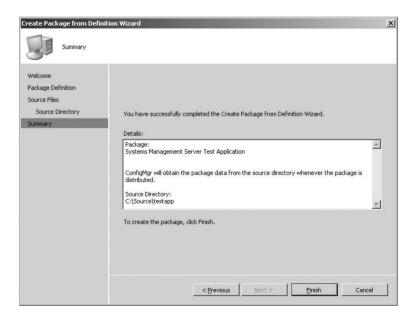


FIGURE 6.37
The Summary page of the Create Package From Definition Wizard



You can use the package you created from scratch earlier in the chapter to go through making a program. In the Configuration Manager console, go to System Center Configuration

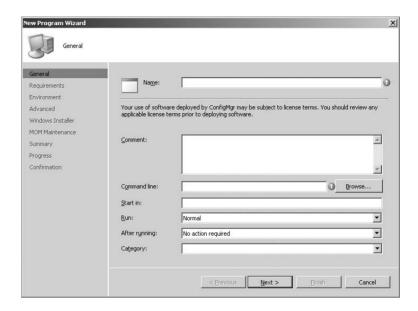
Manager ➤ Site Database ➤ Computer Management ➤ Software Distribution ➤ Package ➤ Microsoft Software Distribution Test Application 1.0.

If you click the Programs node of that package, you will see that it is empty. Right-clicking the Programs node will give you some options, so click New and then Program; this takes you to the General page of the New Program Wizard, shown in Figure 6.38.

FIGURE 6.38

New Program Wizard's

General page



The information that you need to provide is as follows:

Name This is a required field and that must be unique, and it can't be modified. It can be up to 50 characters.

Comment This is optional text and can be up to 127 characters.

Command Line This is a required field; it specifies the command line of the program (for example, setup.exe /a). It can be up to 255 bytes.

Start In This is an optional field that represents the executable folder for the program; it can be up to 127 characters.

Run This sets what mode the program will run in on the client; there are four choices, with Normal being default.

After Running This sets what happens after the program is run; there are four choices, with No Action Required being the default. Those options are as follows:

No Action Required This means Configuration Manager does not need to do anything after the program is complete.

ConfigMgr Restarts Computer The Configuration Manager client restarts the computer automatically.

Program Restarts Computer The program itself restarts the computer after it is finished.

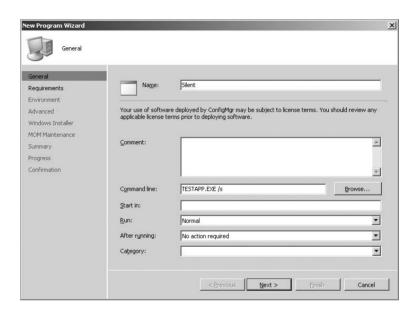
ConfigMgr Logs User Off The currently logged on user is logged out of the computer after the programs finishes.

Category This sets the category that the program will show up under in Add Or Remove Programs. The administrator defines these categories.

In the Command Line field, you will need to browse to where the program for the package is located and select it in the dialog box. If your source is set up correctly, browsing should take you right to it, unless it is in a subdirectory or a command line that is run on the client computer.

Figure 6.39 shows all the fields filled out for the example; you can now click Next to proceed to the Requirements page, shown in Figure 6.40.

FIGURE 6.39
Sample program configuration



The options on the Requirements page are as follows:

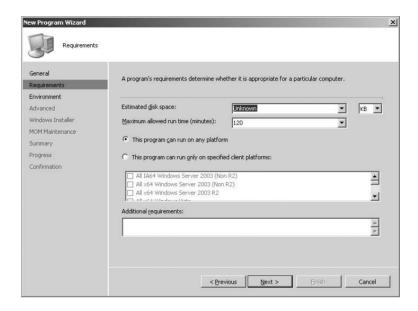
Estimated Disk Space This sets the amount of free disk space that the program will need to run. The default is Unknown but can be set as a whole number greater than or equal to zero. If you do set a value, you will also have to set the value's units.

Maximum Allowed Run Time This sets the maximum time that the program is supposed to run on the client. The default is 120 minutes, but you can set any whole number that is greater than zero. Keep this number in mind if you are deploying to collections with maintenance windows. When a client computer has a maintenance window policy on it, a time evaluation is made before the advertised program will run. This evaluation checks to see whether the available time left in the maintenance window is greater than or equal to the maximum allowed program run time for the program plus the Advertised Programs Client Agent countdown duration (if any). If it is, then the program will run. Otherwise, Configuration Manager will wait for a time when there is enough time to run the program.

This Program Can Run On Any Platform This sets the option that tells Configuration Manager that the program is operating system and hardware independent. This is the default

setting, and if set, Configuration Manager will not even check for the platform type before it runs the program.

FIGURE 6.40 New Program Wizard's Requirements page



This Program Can Run Only On Specific Platforms This sets that the program can be run only on certain operating systems and processor types. When you select this option, you must select at least one platform from the list below it.

Additional Requirements This is an optional field that can be up to 127 characters. This is used mostly for when the program is set up for use in Add Or Remove Programs.

The default options are fine for our example, so you can click Next to proceed to the Environment page of the New Program Wizard, as shown in Figure 6.41.

Its settings are as follows:

Program Can Run This sets the logon conditions for the program. There are three options:

- Only When A User Is Logged On (This is the default setting.)
- Only When No User Is Logged On
- ◆ Whether Or Not A User Is Logged On

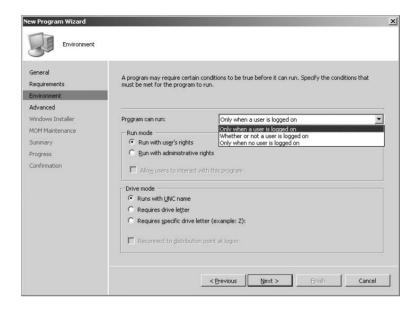
Run Mode This sets what credentials the program is going to use to run the program. There are two options:

Run With User's Rights This is the default and will use the logged on user's rights.

Run With Administrative Rights This setting forces the program to run under the local administrator account on the computer. If you chose this option, another option becomes available: Allow User To Interact With This Program. This check box is available only when

Only When No User Is Logged On is selected as a logon condition and Run With Administrative Rights is selected. Use this combination only if the program requires administrative rights and the user has to interact with the program. Otherwise, leave it blank.

FIGURE 6.41New Program Wizard's Environment page



Drive Mode This section allows you to set how the program handles the drives when it is run from a distribution point. There are three options:

- ◆ Runs With UNC Name (This is the default setting.)
- Requires A Drive Letter (This should be used if the program requires a drive letter to run but it doesn't matter which one is used.)
- Requires Specific Drive Letter (This should be used if the program requires a drive letter to run and it does matter which one is used.)

You can also enable or disable reconnection here:

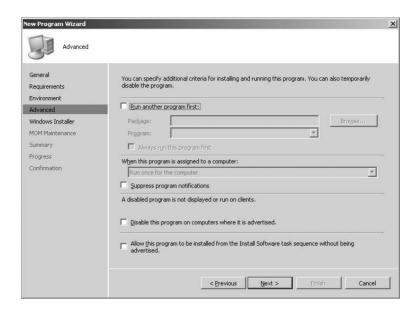
• Reconnect To Distribution Point At Logon (This is unchecked by default.)

For the example, choose Whether Or Not A User Is Logged On, leave everything else at the defaults, and click Next to proceed to the Advanced page of this wizard, shown in Figure 6.42. The Advanced page has the following settings:

Run Another Program First Here you can pick another program that you want to run before this one. This option is deselected by default, and if the program you select here fails when it is run, then the program you are configuring here will not run. If you choose this option, then more options become available that must be filled out.

Package This is the package that has the program that you want to run first.

FIGURE 6.42New Program Wizard's Advanced page



Program This is the program that you want to run before the one you are making.

Always Run This Program First This check box sets the option to have the program specified run every time the advertised program runs, even if it has run before.

When This Program Is Assigned To A Computer Sets how the programs are assigned to users when the Program Can Run option in the previous page is set to Whether Or Not A User Is Logged On. Otherwise, those options are grayed out. When available, those options are as follows:

- Run Once For The Computer
- Run Once For Every User That Logs On

Suppress Program Notifications This option disables all notification messages and countdowns, overriding the site settings if they are enabled. This box is deselected by default.

Disable This Program When It Is Advertised This option temporarily disables access to this program from any advertisements that have it assigned. Any advertisements that assign this program will not run until it is reenabled. This box is deselected by default.

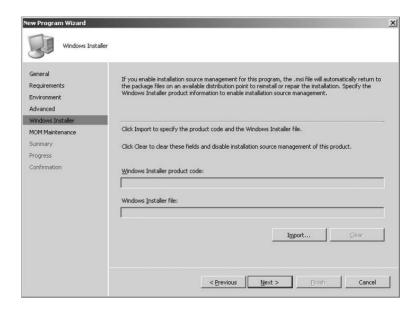
Allow This Program To Be Installed From The Install Program Task Sequence Without Being Advertised This option allows you to use this program with Install Software tasks for use in operating system deployment, without having to be advertised to a collection.

You don't need any of these options for our example, so click Next.

The Windows Installer page of the wizard, shown in Figure 6.43, allows you to import Windows Installer information and have it updated automatically by Configuration Manager. When you import Windows Installer information in this way, Configuration Manager will automatically update the Windows Installer databases on Configuration Manager clients with a list of distribution points that have a copy of the source files for use on the client. This is a great feature that was

introduced in SMS 2003, and it allows Windows Installer installations to be upgraded or repaired more easily, while keeping the source files in one location.

FIGURE 6.43New Program Wizard's Windows Installer page



This page has two fields; the first one is updated only when you import an .msi file through the Import button on the second field. You can import only one Windows Installer source per program in a package. Not all installs can use Windows Installer technology, so you might not be able to use this in every case. In this example, you don't need to use this field, so you can click Next.

Figure 6.44 shows the MOM Maintenance Mode page, which allows you to set a couple of options for computers that are managed by Microsoft Operations Manager (MOM) and might generate alerts because of activity during the program.

The options are as follows:

Disable MOM Alerts While This Program Runs Choosing this option puts the computer in maintenance mode while the program runs, so it will not generate any MOM alerts.

Generate MOM Alert If This Program Fails This option sets whether MOM will generate an alert if the program fails to run properly. If this happens, the alert will have the package name, program name, advertisement ID, advertisement comment, and failure code of the failed program.

These options aren't needed in this example either, so you can click Next.

As usual, the wizard ends with a Summary page (Figure 6.45), which allows you to look over the changes you made and make sure they are right before you finish. If everything looks OK here, you can click Next.

You will see a progress bar that shows your progress, which could take a while depending your hardware resources on the server. When it is done, you see the Confirmation page (Figure 6.46), and you can click Close to finish.

FIGURE 6.44 New Program Wizard page's MOM Maintenance Mode page

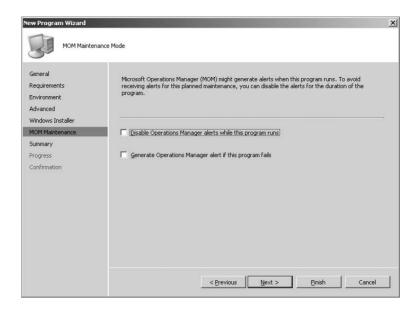
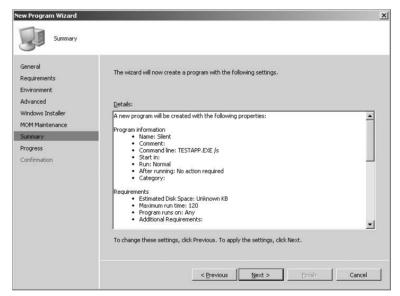


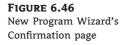
FIGURE 6.45 New Program Wizard's Summary page

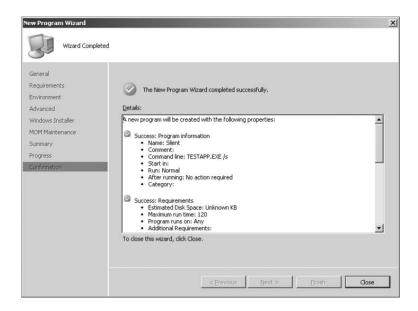


Configuring Distribution Points

As introduced earlier in the chapter, distribution points are site servers or shares that store files for packages so they can be used to be run on client computers. These files can be run either from the distribution point over the network or locally after the files have been downloaded to the client computer.

With the examples in this chapter, we have already shown how to create a package and a program that you can use to test your software distribution system, but before you can deploy the





test program, you will need to add your package to at least one distribution point so clients can access it.

To do that, you go to the Configuration Manager console and navigate to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Distribution ➤ Packages. From there you find the package that you want to distribute, which in this case is named Microsoft Software Distribution Test Application. You can then expand that package to reveal more nodes underneath it. The one you want is Distribution Points, so right-click that, and choose New Distribution Points. This opens the New Distribution Points Wizard.

After quickly reading the welcome text, you can click Next to proceed to the Copy Package page, shown in Figure 6.47.

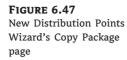
This page lists all the available distribution points, which in this case is just one. After selecting Select All, you can click Next.

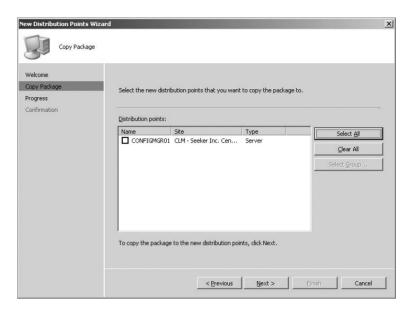
When you do that, you will see a progress dialog box, which might take a while depending on how many sites you are sending the package to and depending on the hardware resources of your Configuration Manager server. Finally, you will see the Confirmation page of the wizard.

This page lets you know whether there are any errors. If there aren't, click Close. To see whether your package has copied to all your distribution points, go further down past the Programs node, and you will see a package status report just for this package. This will tell you whether the package made it to its distribution points or whether there were any problems along the way. This is a new feature for Configuration Manager.

In our example, we set up our test application on the default distribution point that was installed as part of the Configuration Manager install. For almost all your other software deployments, more distribution points are going to be necessary, so we will go over setting up a distribution point on a Configuration Manager site system and on a computer share.

Adding a new server to be used as a distribution point is relatively easy, because the New Site System Server Wizard does all the work. To get there, you navigate in the Configuration Manager console to System Center Configuration Manager > Site Database > Site Management >





site name ➤ Site Settings. Then right-click Site Systems, choose New, and choose either Server or Server Share, depending on what you need for the task.

MAKING A SERVER SHARE AS A DISTRIBUTION POINT

First let's make a server share as a distribution point. After clicking Server Share from the options just shown, you'll see the New Site System Server Share Wizard, as shown in Figure 6.48.

The General page of this wizard has the following options:

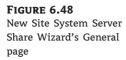
Name Input the path of the new server share site system.

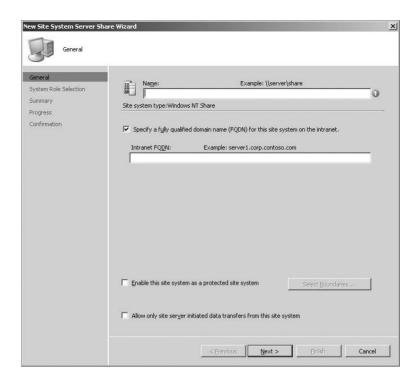
Specify A Fully Qualified Domain Name (FQDN) For This Site System On The Intranet This enables or disables the intranet FQDN text box, which allows you to set an FQDN for the system hosting the share. This is required for many scenarios in Configuration Manager including but not limited to the following:

- Automatic approval of trusted clients in Mixed mode
- ◆ Native mode if the site system PKI certificate uses FQDN
- Environments that have multiple domains and don't use WINS

Intranet FQDN Enter an FQDN for your site system on the intranet. This can be the same as the FQDN from the server's configuration, or it can be a CNAME (alias) on the intranet DNS. If the site is in Native mode, the FQDN must be the same as specified in the server's certificate subject name. The FQDN rules are as follows:

- ◆ Labels can contain ASCII letters, digits, and the hyphen (-) character.
- Labels can't be all numbers but can have a leading digit.
- Labels must end and begin only with a letter or a digit.





Keep in mind that Configuration Manager can't validate what you input here, so double-check your spelling before you continue.

Enable This System As A Protected Site System This option configures the site system as protected, and you must click the Select Boundaries button to open the Boundaries dialog box and choose the boundaries so you can limit client collections to this site system. This option is available only for distribution points and state migration points and can't be set up for clients over the Internet.

Allow Only Site Server Initiated Data Transfers From This Site System By default, site systems make connections to the site server to send status information to its controlling site. With this option enabled, the site server only makes connections to the site. This configuration may introduce some latency in sending status messages and decrease performance on the site server. The following roles support this option:

- Management point
- ◆ Distribution point
- Software update point
- ◆ Fallback status point

Use this option only if the site system servers are in different AD forests than the site server and you need to control those connections. This would more than likely be used when the site is configured for use with Internet-based clients.

Keep in mind that you will have to use the site system installation account with this option, because the site server's computer account will not work.

The last two options on this page aren't needed for this example, so after filling out the required information, you can click Next to proceed to the System Role Selection page. As Figure 6.49 shows, in this case it has only the Distribution Point option. You can select that option and then click Next to complete your selections in this wizard.

FIGURE 6.49
New Site System Server
Share Wizard's System
Role Selection page

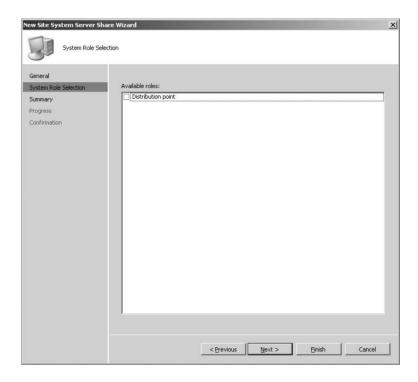


Figure 6.50 shows the Summary page, where as usual you can review the options you have picked and go back change to anything you need to change. Everything seems fine here, so click Next.

A Confirmation page lets you know that everything was successful, so you can click Close to finish.

MAKING A SERVER A DISTRIBUTION POINT

To make a server a distribution point, you start just as you did in the previous example. Go to the Configuration Manager console, and choose System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ site name ➤ Site Settings. Then right-click Site Systems, choose New, and this time select Server.

Figure 6.51 shows the start of the New Site System Server Wizard, at the General page. You will become familiar with this wizard quickly, because it is used to set up all site roles for Configuration Manager. Some of the options on this page are identical to those outlined for a system share.

FIGURE 6.50 New Site System Server Share Wizard's Summary page

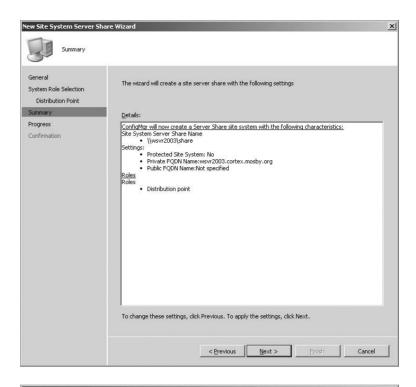
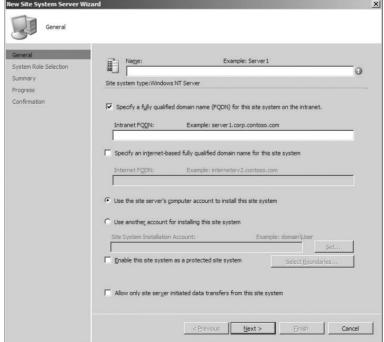


FIGURE 6.51New Site System Server Wizard's General page



The following options are unique to the New Site System Server Wizard:

Use The Site Server's Computer Account To Install This Site System The following option should be selected if the following is true:

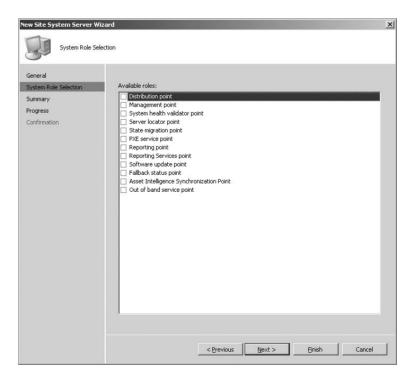
- The site system to be configured is in the same Active Directory (AD) forest as the site server.
- ◆ The site system is in a different AD forest, but there is a trust between the two forests.
- There is an external trust in place where the site system's domain trusts the site server's domain.

If there is no trust in place, you will have to use a Windows user account that is trusted on the site system's server.

Site System Installation Account This field is where you enter the Windows user account, if a computer account will not work. Clicking this option will open the field, and you can click Set to enter the account in the *domain/user* format. In our example, you need to enter a name and an FQDN only; the rest of the options don't apply, so you can click Next.

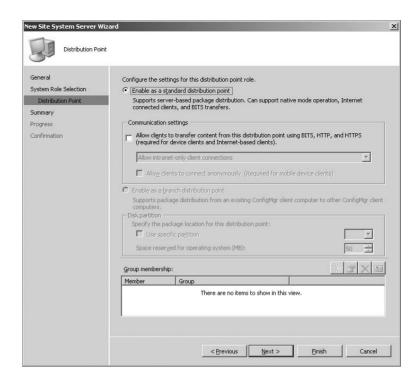
Figure 6.52 shows you the System Role Selection page, and you can see the various roles that are available to choose from, which were discussed in Chapter 3.

FIGURE 6.52 New Site System Server Wizard's System Role Selection page



Choosing Distribution Points opens the options shown in Figure 6.53 (some are grayed out because the server we are using doesn't meet the criteria).





There are only a few options you can configure in this example:

Allow Clients To Transfer Content From This Distribution Point Using BITS, HTTP, Or HTTPS This sets whether clients connecting to this distribution point can transfer files using BITS, HTTP, or HTTPS. This option must be selected to enable BITS network throttling. When you click this option, another one becomes available:

Allow Clients To Connect Anonymously (Required For Mobile Device Clients) Mobile devices require this setting when the site is configured in Mixed mode and is not available in Native mode.

Group Membership This box shows the distribution point groups available on your Configuration Manager site and lets you know whether this distribution point belongs to them.

For this example, select the first check box, and leave all other options on their defaults. (Options that are grayed out are discussed later in the chapter.) From here, you can click Next. That takes you to the Summary page, similar to those you have seen in earlier parts of the chapter. Everything looks good here, so you can click Next, or Finish if you are done configuring options, to finish.

CREATING A BRANCH DISTRIBUTION POINT

Creating a branch distribution point starts exactly like setting up a regular distribution point. In the Configuration Manager console, choose System Center Configuration Manager ➤ Site

Database ➤ Site Management ➤ site name ➤ Site Settings. Then-right-click Site Systems, click New, and select Server.

You will first see the General page, as shown in Figure 6.48 earlier in this chapter, with the fields that were outlined for the New Site System Server Share Wizard. For the example here, you can just fill in the first two fields and click Next.

You are then shown the Systems Role Selection page like you saw in Figure 6.52, and you select Distribution Point to continue. This brings you to the Distribution Point page in the wizard, as shown in Figure 6.54.

FIGURE 6.54
Branch distribution point options

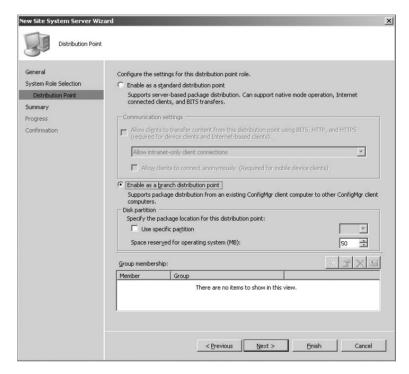


Figure 6.54 gives you some new options that you haven't seen before. If you select Enable As A Branch Distribution Point, since that is what you want to do here, you see the options that were grayed out earlier. As you can see in the Disk Partition section, you can specify which drive you want packages to be stored on, and you can set how much drive space you want to reserve for operating system operations. If this system is not going to be anything but a branch distribution point, then the default setting of 50 MB might be OK, but we recommend increasing it to about 512 MB (depending on your free space available) just in case. It is easier to reduce this number if you need to later than it is to increase it if the hard drive is full of packages.

After clicking Next, you will see the Summary, Progress, and Confirmation pages that you have already become familiar with.

Creating Advertisements

Now that you have created your package and a program for the package and sent the package to a distribution point, we'll show how to make an advertisement to send the test application to your clients and to test your software distribution system.

To get a program to run on a client, you set up an advertisement that sends the package and program information to a collection of clients that you want to run that program. As introduced earlier in this chapter, an advertisement has the following information:

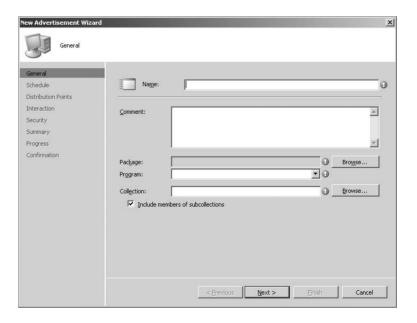
- ◆ Which program is to run on the client.
- ♦ Which collection of computers, users, or user groups will get the program.
- When the program will be available to clients, for how long, or if the program will be mandatory. You can also set up Wake On LAN to be enabled for the advertisement, as well as if the program is important enough to ignore any maintenance windows that a collection might have.

Once again we will take a second to remind you that it is crucial to test any piece of software that you are going to send out through software distribution, before deploying it to any of your clients. A test lab environment is ideal for this kind of testing.

To create an advertisement, you start in the Configuration Manager console and go to the software distribution node under Configuration Management. Then right-click Advertisements, select New, and then select Advertisement.

Figure 6.55 shows you the General page of the New Advertisement Wizard, which asks for the first items of information that you will need to set things up.

FIGURE 6.55New Advertisement Wizard's General page



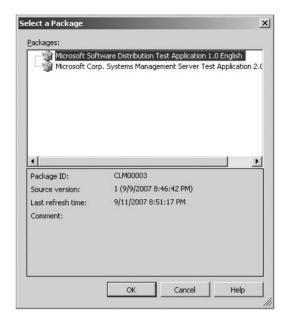
The fields are as follows:

Name This is the name of the advertisement, which is required; it can be up to 100 characters.

Comment This is optional text that can describe the advertisement; it can be up to 127 characters.

Package This allows you to choose the package that has the program that you want to deploy to clients; it's a required field. Click the Browse button to open the Select A Package dialog box (Figure 6.56), and choose which package you want.

FIGURE 6.56
The Select A Package dialog box



Program This specifies the program, from the package you select, that you want to advertise. This is also a required field.

Collection This sets the existing collection that you want to send the advertisement. This is also a required field. Click the Browse button to open the Browse Collection (Figure 6.57) dialog box, which lets you look for the collection you want.

FIGURE 6.57
The Browse Collection dialog box

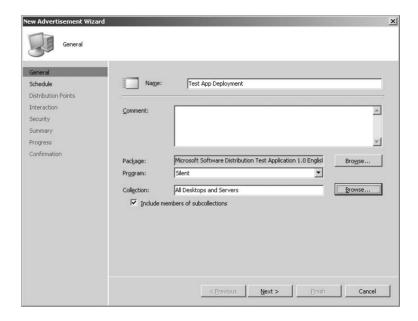


Include Members Of Subcollections This specifies that the program will also be advertised to the clients and users in the selected collection's subcollections. This is selected by default, so you will have to deselect it if you don't want to deploy to subcollections

Figure 6.58 shows the General page after we have filled out the information for Test App. You can click Next to proceed to the Schedule page.

FIGURE 6.58

New Advertisement Wizard's General page after options are filled out



As shown in Figure 6.59, the Schedule page provides options to schedule your advertisement for deployment.

This page has the following fields:

Advertisement Start Time This sets the date and time that the program will be advertised and ready to run on clients in their time zones; it is set to the current date and time by default. To choose another time, just click the arrows next to the value. If an advertisement starts earlier than the mandatory assignment time, the client will download the package at that time. To base the start date and time on UTC time instead of local time, select the UTC box.

Advertisement Will Expire This sets whether you want the advertisement to expire, along with the date and time that it should expire and the program will no longer be able to run. By default, that time is set to six months in advance from the current time if the box is checked. To choose another time, just click the arrow next to the value. To use UTC time for the expire date, just select the UTC box.

Mandatory Assignments This allows you to set up mandatory assignments for this advertisement, of which you can have a maximum of 15. Clicking the New icon opens the Advertisement Schedule dialog box (Figure 6.60). Setting a Mandatory assignment opens up other options (Figure 6.61).

Enable Wake On LAN This specifies whether to have the advertised program wake up the client computer at the time of the mandatory assignment to run the advertised program.

FIGURE 6.59New Advertisement Wizard's Schedule page

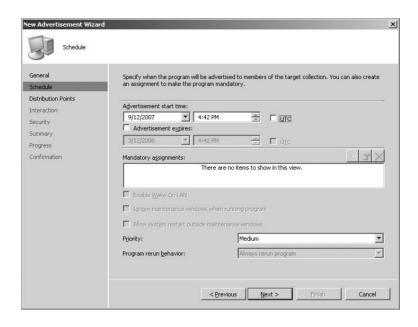
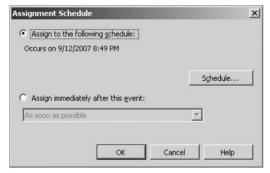


FIGURE 6.60 Assignment schedule



Ignore Maintenance Windows When Running Program This specifies whether to have the advertised program ignore system maintenance windows while the program is running.

Allow System Restart Outside Maintenance Windows This specifies whether to allow a restart (if the program has the Configuration Manager Restarts Computer option enabled) of a client system if the restart would occur outside a preset maintenance window.

Priority This sets the advertisements priority when it's sent to child sites. Low, Medium (default), and High are the options.

Program Rerun Behavior This specifies whether the advertised program will rerun on the client if it has been run before the mandatory time, which will apply even it was run from another advertisement. The following options are available:

- Never Rerun The Advertise Program
- Always Rerun Program (default if not mandatory)

- Rerun If Failed Previous Attempt
- Rerun If Succeeded On Previous Attempt

Figure 6.61 shows what the Schedule page looks like after a mandatory assignment has been entered. For this example, all the default settings are fine, so you can click Next and continue.

FIGURE 6.61 Assignment schedule options with mandatory assignment

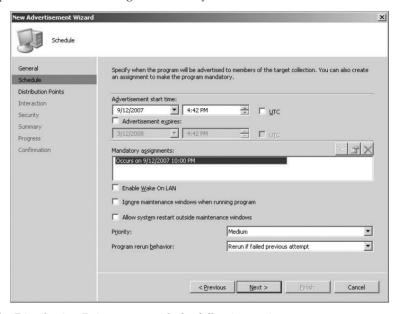
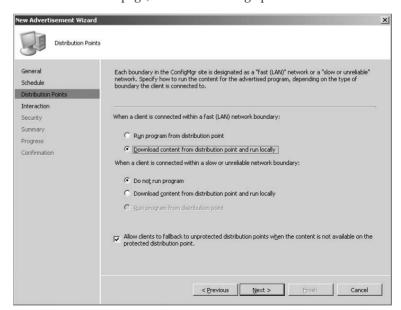


Figure 6.62 shows the Distribution Points page, with the following options.

FIGURE 6.62
Distribution Points page



When A Client Is Connected Within A Fast (LAN) Network Boundary This specifies the options available when the client is within a fast network boundary, with the following options:

- Run Program From The Distribution Point
- Download Content From Distribution Point And Run Locally

This specifies whether an advertised program is downloaded to the client computer before Configuration Manager runs the program when connected within a fast (LAN) network boundary. If the distribution point supports BITS, you can use this setting to ensure the safe download of the advertised program. In the event of the download being stopped, BITS resumes the download the next time the computer connects to the network. (This is the default option; see "Microsoft's New Security Recommendations on Package Security.")

Allow Clients To Fallback To Unprotected Distribution Points When The Content Is Not Available On The Protect Distribution Point This is pretty self-explanatory and probably will be used only for emergencies because it will cause an increase in traffic on the network.

MICROSOFT'S NEW SECURITY RECOMMENDATIONS ON PACKAGE SECURITY

Microsoft now has a new recommendation on the security of advertisements. The Configuration Manager documentation states this:

Selecting the "Download content from distribution point and run locally" option is strongly recommended for greatest security. When this option is selected, the package is hashed so that Configuration Manager 2007 can ensure package integrity. When the "Run program from distribution point" option is selected, the package hash is not verified prior to running the specified program. Therefore, package integrity cannot be ensured as it is possible for users with administrative rights to alter or tamper with package contents.

Besides, if you have users with enough administrative rights that they can modify packages on your distribution points, you have a lot more problems to worry about than advertisement security.

In any case, be aware of these new defaults so they won't cause you any extra trouble.

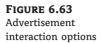
For this example, all the defaults are fine, so you can click Next to continue. Figure 6.63 shows you the Interaction page, which gives you the following options.

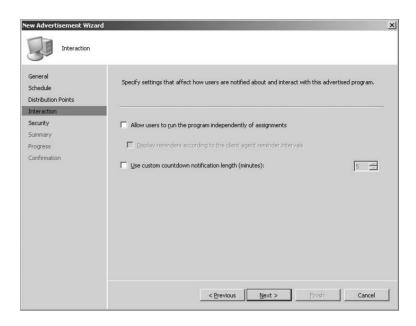
Allow Users To Run The Program Independently Of Assignments This specifies whether users may run the advertised programs on their own and is deselected by default.

Display Reminders According To The Client Reminder Intervals This specifies whether advertisements are broadcast to the client according to the default intervals. This option is available if the previous option is selected.

Use Custom Countdown Notification Length (Minutes) This specifies whether client notifications are broadcast based on a custom notification length in minutes. When selected, you have to set that custom time.

The example doesn't need any of these options, so you can leave them as they are and click Next to continue.





Clicking Next takes you to a Security page like others you have seen in this chapter. From there you get the standard Summary, Progress, and Confirmation pages you have seen before.

There you go! You have sent out your first advertisement to your clients, completing the five general steps of the software distribution process, after creating a collection, package, and program and choosing distribution points.

Monitoring Software Distribution Status

After you set up an advertisement to deploy software, you will need to monitor the process and verify the results. You can perform these tasks in three ways: using the software distribution reports in Configuration Manager, using the Status Message Viewer, and using log files. Each of these shows the results in different ways. After you review the following sections, you can decide which method suits your needs the best.

Using Software Distribution Reports

Out of the box, Configuration Manager includes numerous reports that can be used to monitor software distribution status. In fact, a whole section is dedicated to advertisement status that you can use to actively monitor the status of any software deployment that you have running through Configuration Manager.

Those reports are by far the easiest method to track software deployments, because they are easy to set up and use. You can even share these reports with others, such as with management staff members who don't have rights to the main Configuration Manager functions themselves.

The following is a list of software distribution reports sorted by category:

Software Distribution: Advertisement Status

Advertisement Status Messages for a Client Being Upgraded to the Advanced Client

- Advertisement Status Messages for a Particular Client and Advertisement
- All System Resource Advertisements with Status
- All System Resources for a Specific Advanced Client Distribution in a Specific State
- ◆ All System Resources for a Specific Advertisement in a Specific State
- Chart: Hourly Advertisement Completion Status
- Status of a Specific Advertisement
- Status of an Advanced Client Distribution

Software Distribution: Advertisements

- All Advertisements
- All Advertisements for a Specific Collection
- All Advertisements for a Specific Computer
- All Advertisements for a Specific Package

Software Distribution: Collections

- All Collections
- All Resources in a Specific Collection
- Maintenance Windows Available to a Particular Client

Software Distribution: Packages

- All Active Package Distributions
- All Distribution Points
- All Packages
- All Packages on a Specific Distribution Point
- All Status Messages for a Specific Package on a Specific Distribution Point
- Distribution Status of a Specific Package

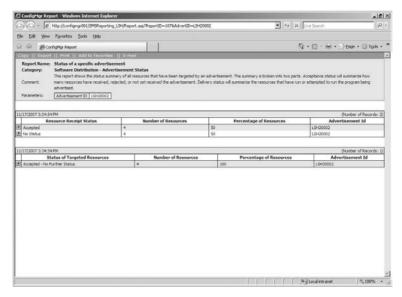
As you can see from the reports in this list, there are categories that cover the different aspects of software distribution, giving you several avenues for monitoring and even troubleshooting software distribution as a whole.

Probably the most useful of these reports for monitoring the success of a software deployment is Status of a Specific Advertisement. This report gives a detailed rundown of a software distribution in two parts. The first is the number and percentage of the targeted resources that have received an advertisement, and the second is the success rate of those resources that received the advertisement in running the deployed software. Figure 6.64 shows this report in various stages of a software deployment.

On the far left of each line that lists a specific status, you can see a shortcut symbol that, when clicked, will drill down to another report that will show even more detail on the resources of any status. Figure 6.65 gives examples of that level of the reports.

FIGURE 6.64

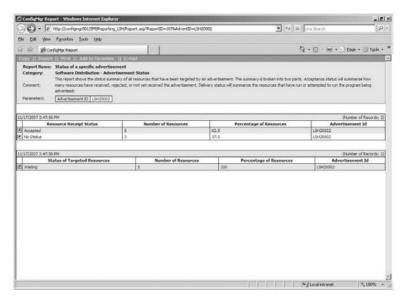
Sample Status of a Specific Advertisement report: (a) main report; (b) detail on systems with no advertisement status; (c) main report after time has passed, showing clients waiting to run advertisement; and (d) main report showing some clients have run the advertisement successfully



(a)



FIGURE 6.64 (continued)

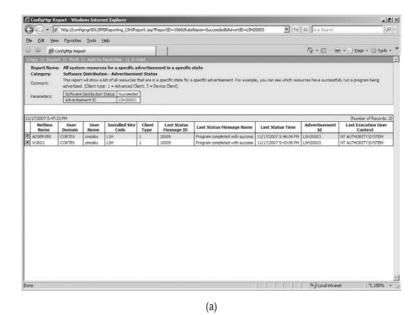


(c)



FIGURE 6.65

Sample Status of a Specific Advertisement report, showing (a) the detail of clients that ran advertisement successfully and (b) the detail of particular client advertisement status



Confighty Report - Windows Internet Deplace

| Part | Part

(b)

Drilling down further from there, you get a report of each stage of a deployment for a particular resource, as shown in Figure 6.66.

You can drill even further down from here if you need to, getting the specific details on a particular status type in the deployment process, as shown in Figure 6.67.

FIGURE 6.66Detail of particular status message

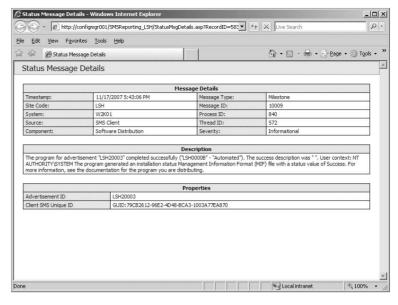
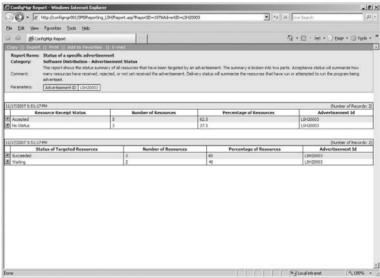


FIGURE 6.67 Status report further along in the advertisement process



During a software distribution deployment, a resource can have any of the following states:

Accepted

Accepted — No Further Status

Cancelled

Download Complete

Download in Progress

Expired

Failed

No Status

Reboot Pending

Retrying

Running

Succeeded

Waiting

Will Not Rerun

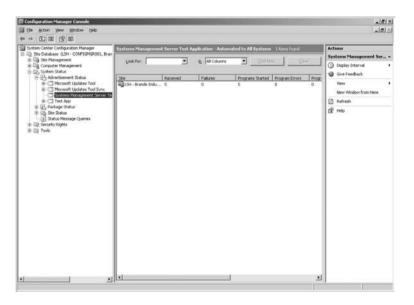
Using the Status Message Viewer

Another way to monitor a software deployment is to use the Status Message Viewer from the Configuration Manager console.

You can access this in a couple of ways, the first being the System Status node. To get there, just go to System Center Configuration Manager ➤ Site Database ➤ System Status ➤ Advertisement Status, and click the advertisement that you want to check.

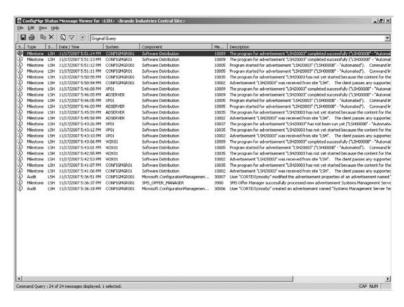
When you select the advertisement you want, you will see several columns in the middle pane that will give you a quick status of that advertisement, as shown in Figure 6.68.

FIGURE 6.68
View of advertisement status from the Configuration Manager console



Depending on your screen resolution, you might have to scroll the middle pane from right to left to see all the columns. If you want more detail on this advertisement, just right-click the information in the middle pane, and select Show Messages followed by the kind of details you want. Figure 6.69 shows an example of choosing All.

FIGURE 6.69
View of Status Message
Viewer when you choose
All



Choosing All displays status messages for the entire advertisement, from messages showing the advertisement's creation all the way down to each target machine either running the deployed program or showing errors if there are any.

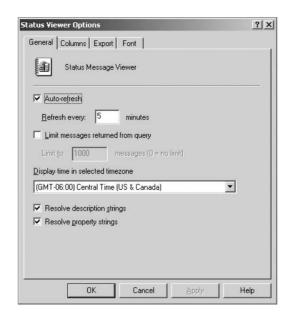
Double-clicking any of the lines in viewer opens up a dialog box that summarizes all the details of that line, as shown in Figure 6.70.

FIGURE 6.70 Status Message Details dialog box



This information is the same as what you would get if you drilled down as far as you could go in the Status of a Specific Advertisement report. The difference here is that you can set the Status Message Viewer to autorefresh every so often on its own. You can do this by choosing View > Options in the Status Message Viewer menu and then opening the General tab, as shown in Figure 6.71.

FIGURE 6.71 The General tab of the Status Viewer Options dialog box



From there you can set the viewer to autorefresh, and you can choose the time between refreshes and other options.

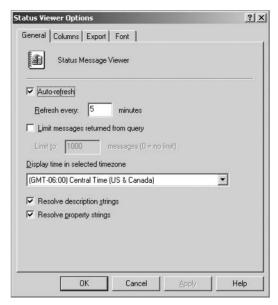
You can also get to a similar view of status messages in the Status Message Queries node. Under that node, several specific status message queries pertain to software distribution:

- ◆ Advertisements Created, Modified, Or Deleted
- ◆ All Status Messages For A Specific Advertisement At A Specific Site
- All Status Messages For A Specific Package at a Specific Site
- ◆ Clients That Failed To Run A Specific Advertised Program Successfully
- Clients That Failed To Start A Specific Advertised Program
- ◆ Clients That Ran A Specific Advertised Program Successfully
- Clients That Received A Specific Advertised Program
- Clients That Rejected A Specific Advertised Program
- Packages Created, Modified, Or Deleted
- Programs Created, Modified, Or Deleted

Now, viewing status messages this way is a little bit more complicated. To start the Status Message Viewer, using the All Status Messages for a Specific Advertisement at a Specific Site query in our example, right-click the query you want to view, and select Show Messages. This displays a dialog box for entering information, as shown in Figure 6.72.

You will have to know the advertisement ID for the advertisement that you want to view and decide on a time frame to get data. If you don't know that advertisement ID, you can always look under the Advertisement node in the Configuration Manager console, where it will be one of the last columns shown in the middle pane.

FIGURE 6.72 Status Message Viewer criteria input



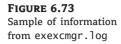
You will also need to have a general idea of the time frame you want to look at; if you define the time frame to be too short (for example, an hour ago), you might not get any data. If you make it too wide (the furthest out you can go is one year), you might get information overload. If you start up the status viewer right after you set up the deployment, you can just set autorefresh and watch the status messages flow in as they happen. Keep in mind that running too many of these kinds of queries can use up system resources pretty fast, especially if your hardware isn't very robust in the first place.

Using Log Files

The only problem with the methods of monitoring software distribution that we have discussed so far is that you have to wait for the Configuration Manager client to report the advertisement status to its management point and for that status to make it up the chain to your central Configuration Manager site. If something happens along the way, like the client's management point going offline after a deployment is finished, you might not have any status messages at the central site level. In cases like this, you just might have to connect to a client directly and see whether an advertised program has been run successfully.

When you have to go looking for log files on a Configuration Manager client related to software distribution, the one you want to look for is execmgr.log. With this log file, you will find everything you need, such as status on policy retrieval, program download status, and actual status of advertised program execution. A sample of what you will find in this log (in SMS Trace, Trace32.exe, from the Configuration Manager 2007 Toolkit; only Wally Mead still uses Notepad!) appears in Figure 6.73.

With SMS Trace, you can monitor this log file in real time and watch an advertisement run on a client as it happens. If you haven't delved into Configuration Manager logs before now, it might take some getting used to the information you are seeing. If a log scrolls too fast for you to read it, you can always use the Pause button under Help to stop the log flow until you can catch up. The log file output will queue up in SMS Trace until you are ready to continue. After you watch the log for a while, it will make more sense, and you will be able to tell what is going on in no time.







GIVING YOUR MANAGER REPORT ACCESS

You have a big deployment of an upgrade to one of the main applications that you use at your organization. Naturally, your manager is nervous about how things will turn out and has asked you for quick access to a report so that he can monitor the progress of the deployment in case his manager asks how the deployment is going.

To give your manager access to the Status of a Specific Advertisement report, go into the properties of that report (report #107) in the Reporting node of the Configuration Manager console, and make sure that your manager (or a group he belongs to, if there are others who need access to the report) has at the very least Read rights under the Instance security rights for that report. Since he is your manager, he will more than likely need Read rights to all the reports. After you do that, check the SMS Reporting Users local group on your reporting server, and make sure that he is in that group as well.

From there you can input the data into the Status of a Specific Advertisement report for your upgrade distribution and email the link that is produced to your manager. All he has to do now is refresh the report every so often to get an update on the deployment's status.

Virtual Application Packages

As stated earlier in the chapter, Configuration Manager 2007 R2 now supports running sequenced applications that have been created with the Microsoft Application Virtualization Sequencer (not included with Configuration Manager; see "Note on the Microsoft Application Virtualization Platform"). Virtual application packages run on Configuration Manager clients without having to physically install the actual software application on the computer.

NOTE ON THE MICROSOFT APPLICATION VIRTUALIZATION PLATFORM

Although Configuration Manager 2007 R2 supports streaming virtual applications, it does not actually enable you to do so out of the box. To be able to use this feature fully, you have to purchase the Microsoft Application Virtualization (App-V) platform, which is part of the Microsoft Desktop Optimization Pack (MDOP), separately. To qualify to purchase the MDOP, you first need Microsoft Software Assurance (SA), which is also required to purchase the R2 version of Configuration Manager 2007.

For more information on SA, you can go to this website: www.microsoft.com/licensing/sa/default.mspx

For more information on MDOP, go to this website: www.microsoft.com/windows/enterprise/products/mdop.aspx

For more information on App-V, go to this website: www.microsoft.com/windows/enterprise/products/app-virtualization.aspx

Virtual Application Package Terminology

These terms will help you understand the following discussion of Virtual Application Packages:

Microsoft Application Virtualization Platform (App-V) This is a separately purchased product that contains the products used to create, store, distribute, and run sequenced applications. It includes the Microsoft Application Virtualization Sequencer.

Sequenced Application This is an application created by the Microsoft Application Virtualization Sequencer that can then be streamed to a computer with the Microsoft Application Virtualization Terminal Services Client or the Microsoft Application Virtualization Desktop Client.

Sequencing This is the process of creating an application package by using the Microsoft Application Virtualization Sequencer. This is done by monitoring an application, configuring its shortcuts, and then creating the actual application package. This package contains files of the .osd, .sft, .sprj, and .ico file types.

Microsoft Application Virtualization Desktop Client This is the separate client agent that runs on a Configuration Manager client, with Windows XP or higher, that communicates and authenticates with the Configuration Manager 2007 site to get the virtual application package, allowing a sequenced application to be run locally.

Microsoft Application Virtualization Terminal Services Client This is the client agent that runs on a Terminal Server and communicates and authenticates the Configuration Manager 2007 site to get the virtual application package, allowing a sequenced application to be run locally.

Virtual Application Package This is an application virtualization sequenced application that has been imported into Configuration Manager 2007.

Streaming This is the process of running a virtual application package from an Application Virtualization streaming—enabled distribution point.

Application Virtualization streaming—enabled distribution point This is a Configuration Manager 2007 distribution point that has been enabled to stream virtual application packages.

Importing a New Virtual Application Package

To deploy a virtual application package to Configuration Manager clients, you first have to import a Microsoft Application Virtualization sequenced application into Configuration Manager.

Configuration Manager uses the XML file that is created when an application is sequenced to import the Name and Version properties of the virtual application using the New Virtual Application Wizard. That information is then assigned to the imported application properties in Configuration Manager. (You can change this information later if necessary.) The XML file is a file manifest of the virtual application and will also have other information on that package. The .sft filename is changed in the import process, and the linked .osd file is then configured to reference the new .sft file.

Before you begin the import process, you need to create a separate source and destination directory for your imported sequenced application. You can name these directories anything you want. The source directory should have the sequenced application that was created using the Microsoft Application Virtualization Sequencer. The destination directory is where the sequenced application will be saved after it has been imported into Configuration Manager. Make sure that these two directories are different, because all files in the destination folder will be overwritten with new files during the import process.

From there, virtual application packages in the destination folder can then be sent to distribution points that have been enabled for virtual application package use and will show up under the results pane of the Configuration Manager console under the Packages section when the New Virtual Application Package Wizard is complete.

Configuring Configuration Manager Clients to Run Virtual Applications

Before Configuration Manager clients can use virtual applications, you must first enable the Enable Distribution of Virtual Applications to Clients option in the Advertised Programs Client Agent properties, as shown in Figure 6.1.

Next you must then deploy the Microsoft Application Virtualization Client (Windows XP or higher) to any Configuration Manager clients that you want to be able to use virtual application packages. This client is obtained separately as part of the Microsoft Application Virtualization platform.

Configuring Virtual Application Package Streaming

To enable a distribution point for virtual application package streaming, you first must enable the Allow Clients To Transfer Content From This Distribution Point Using BITS, HTTP, And HTTPS setting in the distribution point properties, as shown earlier in Figure 6.53. This will then allow you to select the Enable Virtual Application Streaming option on the Virtual Applications tab of the distribution point properties.

Advertising a Virtual Application Package

You can advertise a virtual application package just like any other package in Configuration Manger 2007, as long as the client has the Microsoft Application Virtualization client installed and is not in a workgroup. For all other intents and purposes, the rest of the process is just like advertising a regular software package.

The Bottom Line

Plan for software distribution Microsoft greatly expanded Configuration Manager's granularity of configuration for software distribution. It now gives an administrator a lot more options for planning and deploying software that meets their business needs.

Master It A branch distribution point (BDP) is designed for small branch offices that have a minimal amount of resources and/or bandwidth at their location. They function a lot like standard distribution points but provide greater control over the scheduling and throttling of network traffic by using BITS. BDPs use BITS like a standard distribution point, but do they require IIS to work?

Create and manage packages Packages are what Configuration Manager uses to send software to clients and are the core of the software distribution feature. Packages can be anything from a full-fledged software install such as Microsoft Office 2007 to a script to change the administrator password on workstations to just a shortcut that you want copied to your user's desktop.

Master It How do you get to the Packages node in the Configuration Manager console?

Create and manage programs Although a package has all the source files or information needed to be sent to client computers, it is the program that actually tells the client what to do with the package files when it is time to run them. Each package should have at least one program and should contain all references to install files, scripts, or command-line switches that are needed to run the program.

Master It What is the default setting for the maximum allowed run time of a program?

Create and manage distribution points Distribution points are site servers or shares that store files for packages so they can be used to be run on client computers. These files can either be run from the distribution point over the network or run locally after the files have been downloaded to the client's cache.

Master It What setting has to be enabled on a distribution point to allow the use of BITS network throttling?

Create and manage collections Collections are an essential part of the software distribution process because they represent groups of resources that are used as targets for software deployments. Collection membership either can be by direct assignment or can be query based. With direct membership, you must manually add the resources that belong to that collection and also manually update that collection as resources are added or deleted. Query-based membership is dynamic, so you do not have to manually manage the resources in the collection, and it is updated automatically on a specific schedule.

Master It On what page of the New Collection Wizard do you configure collection membership?

Create and manage advertisements To get a program to run on a client, you must set up an advertisement that sends the package and program information to a collection of clients that you want to run the program.

Master It What information is sent to clients in an advertisement?

Monitor software deployments The results from software distribution reports are made from direct SQL queries on the Configuration Manager database. They are snapshots of data taken from the time that the report is run.

Master It Which is the best report for viewing the status of an advertisement?

Chapter 7

Software Updates

Ever since the Nimda worm hit the Internet in September 2001, patch management has become a very important part of maintaining network security. That worm brought forward the importance of patch management because it was vulnerabilities in Windows that had allowed the worm to spread so fast around the world, and they were vulnerabilities that Microsoft had released patches for several months earlier.

At the time, patching an operating system was a very labor-intensive task. Windows Update was available, but you still had to run it manually on each machine that needed updates. This meant connecting to the Internet, which was really too dangerous for corporate networks while Nimda was spreading. As a result, network administrators and PC support staff ended up travelling to all their computers with a CD full of updates to get them patched up and safe again.

Microsoft released Software Update Services in 2002, and SMS 2.0 got some patch management functionality through an add-on feature pack. However, it wasn't really until SMS 2003 that there was a real functional patch management solution for the corporate enterprise. SMS 2003 used Microsoft Update technology to detect and install its updates, and it allowed reporting to show the progress. This was not without its problems; as more and more patches became available for Microsoft's operating systems and applications, this patch solution became more taxing on server and workstation resources.

The Software Updates feature in Configuration Manager has been rewritten from the ground up but has made the software update process even more effective by leveraging the Windows Server Update Service (WSUS) product and incorporating its capabilities into patch management and also taking some of the load off Configuration Manager clients in the process.

In this chapter you learn to:

- ◆ Plan to use Software Updates
- Configure Software Updates
- ◆ Use the Software Updates feature to manage software updates

What's New in Software Updates

The Software Updates feature of Configuration Manager now leverages WSUS technology to allow for more granular configuration options, separates itself from dependency from other Configuration Manager features, and finally consolidates client scanning into one tool. The newly designed feature also allows for a wider variety of updates as well as decreasing the amount of bandwidth the feature uses overall.

Table 7.1 gives an overview of the changes to Software Updates in Configuration Manager compared to SMS 2003.

TABLE 7.1: SMS 2003 and Configuration Manager Software Updates Compari

FEATURE	SMS 2003	Configuration Manager
Compliance Assessment	Multiple scanning tools, offline CAB files with update lists.	Uses Windows Update Agent to connect to WSUS on a Configuration Manager Software Update Point.
Update Categories	Security patches, update rollups, service packs, and other non-Microsoft updates.	All Microsoft update and non-Microsoft categories available on Windows Update.
Scan Results	Requires hardware inventory to gather and report scan results.	Results are gathered by state messages, which are faster and more accurate.
Deployments	Uses software distribution packages, programs, and advertisements.	Uses a deployment system separate from software distribution. Deployments don't require direct relationship with deployment packages.
Admin Experience	Admin runs a 17-step wizard every time an update is added or changed. Every language version for every update is included.	Templates can save common settings, search folders, group updates according to any criteria, update lists, speed up deployments and reporting. The console homepage provides a status summary, and language versions can be separated.
Update binaries	Client required to download entire package or run from distribution point (DP).	Client downloads only the missing updates it needs to install.

Prerequisites for Software Updates

Before you can plan and set up Software Updates, you need to be familiar with its components, so you can determine which ones must be installed and configured for your environment. Table 7.2 provides a list of these components.

Of course, you will also need to configure a reporting point before you can use the Software Update reports. We go into more detail on configuring a reporting point in Chapter 11.

UPGRADED ADMINISTRATORS WILL NOT HAVE ACCESS TO NEW SOFTWARE UPDATE OBJECTS

After upgrading an SMS 2003 site to Configuration Manager, only the administrator who did the upgrade will have access to all of the new objects in the Configuration Manager console. Any other administrator will have access only to the objects they had access to in SMS 2003, even if they had full rights before. To get around this issue, make sure that you give rights to any administrators that need this access after the upgrade to Configuration Manager is complete.

TABLE 7.2: External Prerequisites to Configuration Manager Software Updates

Prerequisite	DESCRIPTION
Windows Server Update Services (WSUS) 3.0 SP1	Software Updates requires WSUS 3.0 to be installed before setting up the Software Update point site system role as it is used for update synchronization and compliance assessment on clients.
WSUS 3.0 Administrator Console	The WSUS 3.0 Administrator Console is required on the Configuration Manager site server when WSUS is not on the site server itself. The console is required to communicate with a remote WSUS server.
Windows Update Agent (WUA) 3.0	The WUA 3.0 client is required, in addition to the Configuration Manager client, to connect to the WSUS server so it can retrieve the list of software updates that need to be scanned for.
Network Load Balancing (NLB)	A software update point (SUP) can support up to 25,000 clients, but if you expect to have more clients connecting to the active SUP you can configure it to use an NLB cluster.
Background Intelligent Transfer Server (BITS) 2.5	Microsoft highly recommends that BITS be enabled and configured for a Configuration Manager site and that distribution points also be BITS enabled. Because software updates are downloaded to the local client cache before they are installed, having BITS enabled will allow clients to continue a download of updates if a client is disconnected from a distribution point.
Windows Installer 3.1	Certain updates, like ones for Microsoft Office, require Windows Installer 3.1 or they will not be detected during a scan for compliance. If you were using the ITMU tool for SMS 2003, this requirement has probably already been met.
Site server communication to the active SUP	There may be configuration settings that need to be examined depending on your SUP infrastructure and Configuration Manager settings. We will go into that in more detail in the section on planning the SUP installation.

Elements of Software Updates

Before you can plan to implement the Software Update process, you need to become familiar with the various elements of the process and their roles in the overall picture.

Software Update Point

As discussed in Chapter 4, the *software update point* (SUP) is a new site system role that is required for managing software updates in Configuration Manager. Each Configuration Manager site must have at least one active SUP before it can deploy software updates to Configuration Manager clients. The SUP role can only be configured on a server that already has Windows Update Server Services (WSUS) 3.0 SP1 installed. The Software Update Point software provides the bridge

between the WSUS components and Configuration Manager. It allows synchronization with the WSUS database to download the latest software update information from Microsoft Update, and locally published updates.

When the Software Update Point site system role is created and configured as the active SUP, the SUP components are installed and enabled. The WSUS Control Manager Component configures the associated WSUS server with the settings that were chosen when you set up the Software Update Point site system role.

The SUP settings can be changed from the Software Update Component Properties window via the Configuration Manager console. Go to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ Component Configuration, and then select Software Update Point Components.

The SUP settings can change the active SUP site system server, the active Internet-based SUP site system if one is needed, the synchronization source, the schedule, and the products, classifications, and languages for which software updates with be synced with the database. You will find more details on these settings later in the chapter.

The first time the SUP completes its synchronization; the Software Updates Client Agent components are activated from a dormant state and will connect on a schedule to WSUS on the active Software Update Point server to start a scan for update scan compliance, as described earlier in the chapter.

Software Updates Client Agent

This is now a separate component from Software Distribution. It is enabled by default and is installed along with the other client components when the Configuration Manager client is installed on a computer. The Software Updates Client Agent is now what manages client scan requests for compliance, evaluation requests, deployment policies, and update download requests. Configuration Manager clients don't use Automatic Updates to retrieve or install software updates.

Software Updates Metadata

A software update has two parts: the software updates file(s) and the metadata. The metadata is contained in the Configuration Manager database and provides information about the software update, including its name, description, products supported, update class, KB article ID, download URL, rules that apply, and so on.

Most importantly, the metadata for each software update defines what products are applicable to the update. A product (for example, Windows XP) is a specific edition of an OS or application. A product family (for example, Microsoft Windows) is a base OS or application from which single products come. You can select a product family or individual products when choosing what will be synced by Configuration Manager.

MULTIPLE PRODUCT UPDATES

If an update is applicable to many products and at least a few of those products from a product family have been chosen for synchronization, then all of them will appear in the Configuration Manager console.

The metadata for each update also defines the update's *classification*. This represents the type of software an update will update on clients. There can be many different classifications for any

given product family, which we will go over in the Planning to Use Software Updates in the Configuration Manager section of this chapter. The metadata also defines what languages the update file is applicable to, and it provides a summary for the software update in one or more languages.

Software Update Files

The software update files are the actual files that the client downloads, such as an .exe, a Windows Installer file (.msi), or Windows Installer patch (.mps), and then installs to update a component or application. The software update file might be stored on a WSUS 3.0 server that is configured to be an active SUP, but it is always stored on distribution points for the site when the software update is downloaded or deployed.

Software update files are retrieved from either the upstream server or Microsoft Update. The updates are then copied to DPs when the software update is downloaded using the Download Updates Wizard or deployed to clients using the Deploy Software Updates Wizard. Both methods are covered in detail later in the chapter. Both download the software update files to a temp location on the site server hard drive, which creates and stores a compressed package file containing the software update, decompresses the package file, and then copies the update file to the package share folder on the DP.

Software Update Objects

Each feature listed in the Software Updates tree in the console allows you to create objects. In most cases, class and instance security rights can be configured for the object, and administrative actions can be run against the object to start a process. Table 7.3 shows the software update objects that can be found in the Configuration Manager console.

TABLE 7.3:	Software Update Objects

Овјест	DESCRIPTION
Deployment Management	Used to deploy software update to clients in the target collection. These objects are replicated to child sites, but are read-only.
Deployment Packages	Hosts the software update source files. These objects are replicated to child sites where they are read-only.
Deployment Templates	Stores many of the deployment properties that may not change from one deployment to the next and are used to save time and ensure consistency when creating deployments.
Search Folders	Provides an easy way to retrieve a set of software updates that meet the search criteria.
Software Updates	Every software update has a configuration item object that is created during the software update sync cycle.
Update Lists	A fixed set of software updates that can be used for delegated administration and creating software update deployments.

As noted in some of the preceding descriptions, software update deployment and deployment package objects are replicated from the site where they were created to all child primary sites in

the Configuration Manager hierarchy. The objects replicated to a child site will be read-only. Even though the properties for these objects must be modified at the site where they were created, the actions available for deployments at child sites are the same as the site where they were created. Also, deployment packages can be used to host the software updates that are deployed on the child sites.

Update Lists

An update list in Configuration Manager contains a set of software updates. Update lists offer several benefits for deploying and monitoring software updates, and are part of Microsoft's recommended Software Updates workflow.

Using an update list allows you to delegate the administration of approving and deploying software updates. For example, an administrator (admin) at the central site can select the software updates that need to be deployed and add the updates to an update list. Admins at child sites, with restricted rights to objects, can then use the update list and deploy the updates to the collection that needs them. Table 7.4 describes the minimum rights that an administrator at a child site needs in order to send out a software update deployment when the update list, deployment template, and collection have been created, and when the software updates have been downloaded to a deployment package.

TABLE 7.4:	Minimum	Required	Rights to	Deploy	Software Updates

CONFIGURATION MANAGER OBJECT	READ	DISTRIBUTE	CREATE	Advertise
Collection	Y	N	N	Y
Configuration Items	Y	Y	N	N
Deployment	Y	N	Y	N
Deployment Package	Y	Y	N	N
Deployment Template	Y	N	N	N
Site	Y	N	N	N

Tracking the compliance state for the software updates in deployments is an important task for Configuration Manager admins. If deployments are made without update lists, it's very hard to get the overall compliance state for the same set of software updates that have been sent out with multiple deployments. When update lists are used instead, you can use the Compliance 1 - Update List Overall report for the set of updates in the update list, or the Compliance 3 - Update List (Per Update) report to get a list of the updates in an update list and the overall compliance of each. This is a great reason to use the update lists as a part of your software update procedure.

Deployment Templates

Deployment Templates can store many of the software update deployment properties, and they can be created for consistency, to save time, or to fit your software update procedures. Templates are created prior to deploying updates by running the Deployment Template Wizard, discussed in detail later in the chapter. Table 7.5 shows the deployment properties for a deployment template.

Deployment Template Properties		
SETTING	DESCRIPTION	
Collection	The collection that will be targeted for the software update deployment. This is optional when you make a deployment template.	
Display/Time Settings	Sets whether the user will be notified of pending updates, the installation progress for updates, whether the client evaluates the deployment schedule in local or Coordinated Universal Time (UTC), and the time frame between when an update is available and when it is mandatory on clients.	
Restart Settings	Sets the system restart behavior when an update installs on a client and needs to restart to finish. Also, allows a system restart to be completed outside of a maintenance window.	
Event Generation	Sets whether Microsoft Operations Manager (MOM) alerts are disabled while updates install and/or sends an alert if the install fails.	
Download Settings	Sets how clients will interact with the distribution points when they get a software update deployment.	
SMS 2003 settings	Sets whether you want to deploy updates to any SMS 2003 clients that could be in a target collection.	

Creating deployment templates in advance for typical deployment scenarios in your environment allows you to create deployments using templates that populate many of the properties that are most often static for the particular deployment scenario. Using the deployment template also reduces the number of wizard pages to work through in the Deploy Software Update Wizard by up to seven pages, depending on what information you have already populated. This not only saves time but also helps to prevent mistakes when setting up a deployment.

Deployment Packages

A *deployment package* is the method used to download software updates (either one or several) to a network shared folder, which must be manually created before it is used, and copy the software updates source file to distribution points defined in the deployment.

Software updates can be downloaded and added to deployment packages prior to deploying them by using the Download Updates Wizard. This wizard provides admins with the capability to provision software updates on distribution points and verify that this part of the deployment process works properly.

When downloaded software updates are deployed using the Deploy Software Updates Wizard, the deployment automatically uses the deployment package that contains each software update. When software updates are selected that haven't been downloaded or deployed, a new or existing deployment package must be specified in the Deploy Software Updates Wizard, and the updates are downloaded to the package when the wizard is finished.

There is no hard link between a deployment and a specific deployment package. Clients will install software updates in a deployment by using any DP that has the software updates, regardless of the deployment package. Even if a deployment package is deleted for an active deployment, clients will still be able to install the software updates in the deployment — as long as each update

has been defined in at least one other deployment package and is present on a DP that the client can get to. To help prevent software update deployment failures, you should then make sure that deployment packages are sent to a group of DPs that can be accessed by all the clients you are targeting.

Deployment package access accounts allow you to set permissions to specify users and user groups that can access a deployment package folder on DPs. Configuration Manager makes these folders available to everyone by default, but you can modify this access if it is required for a specific security need.

Configuration Manager 2007 client computers also have the option of selective download: a deployment package might contain both updates that are required for a client and some that are not, but the client can determine which software updates are applicable and retrieve only those files. This allows admins the choice to have multiple updates in a single deployment package and use it to target clients that might need only some of those updates. Selective download is not available on SMS 2003 clients, and they must download the entire package before they can install any of its files.

Deployments

While it is deployment packages that host the update files, it is *software update deployments* that actually deliver software updates to clients. The Deploy Software Update Wizard is used to create deployments and can be started using several methods, which we will detail later in the chapter. Table 7.6 lists all the pages in this wizard and describes the settings that can be configured in each one to create a software update deployment.

If an update in a deployment has Microsoft Software License Terms that have not been accepted yet, then a Review/Accept License Terms dialog box will appear before the Deploy Software Updates Wizard, and give you a chance to review and accept the license terms. When you accept the terms, then you can deploy the updates. If you don't accept the terms, the process is cancelled.

System Center Update Publisher

The System Center Updates Publisher has been built on the custom updates framework that was introduced in Systems Management Server 2003 R2. Updates Publisher is a standalone tool that enables independent software vendors or line-of-business developers to import custom software update catalogs, create and modify software update definitions, export update definitions to catalogs, and publish software update information to a configured WSUS server. By using Updates Publisher to define software updates and publish them to the WSUS server, the Software Updates feature in Configuration Manager is able to synchronize the custom update from the WSUS server database to the site server database. This will allow you to enable client computers to scan for custom update compliance, and to provide administrators the ability to deploy the custom updates to client computers.

The Software Update Process in Configuration Manager

As you'll see throughout the hands-on portions of this chapter, the biggest parts of the software update process are planning and configuration. After those have been completed, there are three main operational phases that are performed by Configuration Manager itself: synchronization, scanning for compliance, and deployment.

TABLE 7.6: Software Update Deployment Wizard Settings		Update Deployment Wizard Settings
	PAGE	DESCRIPTION
	General	The name and description of the deployment.
	Collection	The collection that will be targeted for the software update deployment. This is optional for a deployment template.
	Display/Time Settings	Sets whether the user will be notified of pending updates and/or the installation progress for updates, if the client evaluates the deployment schedule in local or Coordinated Universal Time (UTC), and the time frame between when an update is available and when it is mandatory on clients.
	Restart Settings	The system restart behavior when an update installs on a client and needs to restart to finish.
	Event Generation	Sets if Microsoft Operations Manager (MOM) alerts are disabled while updates install and whether to send an alert if the install fails.
	Download Settings	Sets how clients will interact with the distribution points when they get a software update deployment.
	SMS 2003 settings	Sets whether you want to deploy updates to any SMS 2003 clients that could be in a target collection. $$
	Deployment Package	The deployment package that will host the software updates for the deployment. This setting won't show up if the updates have already been downloaded to a package.
	Download Location	Lets you choose to download the updates from the Internet or from a source on the local network.
	Languages Selection	The languages for which the software updates that will be in the deployment are downloaded.
	Deployment Schedule	The schedule for when an update deployments is active, when update installs are enforced, if Wake On LAN is enabled, and if you are going to ignore maintenance windows when updates are installed.
	NAP Evaluation	If the software update in this deployment will be added in a Network Access

Synchronization

This is the process of retrieving the metadata for software updates that meet the configured criteria; it can be retrieved from either the upstream Windows Server Update Services (WSUS) 3.0 SP1 server or Microsoft Update. The WSUS Synchronization Manager component on the SUP works with WSUS to complete the synchronization process. The highest site in

Protection (NAP) evaluation.

the Configuration Manager hierarchy (the central site in most cases) that has an active SUP synchronizes with Microsoft Update; this is done either on a schedule you set up or manually by using the Run Synchronization action on the Update Repository node in the Configuration Manager console. (We go into more detail on how to do that later in the chapter.) When a sync cycle is started at the central site, the WSUS Synchronization Manager makes a request to the WSUS service to start a sync cycle. The software update's metadata is then synchronized from Microsoft Update and any changes are inserted into the WSUS database.

When WSUS finishes its sync cycle, WSUS Synchronization Manager starts syncing with the WSUS database and inserts any changes into the site server database. When that process is finished, the WSUS Synchronization Manager component (SMS_WSUS_SYNC_MANAGER) creates a status message with an ID of 6702.

DIFFERENCE BETWEEN SCHEDULED AND MANUAL SYNCHRONIZATION

A scheduled synchronization does a full sync, but using the Run Synchronization action does only a delta sync. Updates are marked as expired if they are superseded by another software update or marked as expired in the update catalog. They are only marked as expired during the scheduled synchronization.

When a sync is run on a schedule, all changes to the software update metadata since the last scheduled sync are put into the site database. This includes metadata that is new (products, languages, and so on), modified, or removed. A manually run sync will be faster than a scheduled one because it is only downloading delta changes to what already exists in the database.

When a software update sync finishes at the central site, a sync request is sent out to all of its child sites. When a child site gets that request, it will first sync itself from its parent site and then send out a request to any child sites that are configured as SUPs. This continues on down the hierarchy until all child sites have been synchronized.

With an active Internet-based SUP (which is used in Network Access Protection scenarios), a sync request is sent to it right after the active SUP is finished with its syncing request. The process for both is the same except that the upstream server of the Internet-based SUP is automatically configured to be the active SUP for the site, and the site server database is not updated when the Internet-based SUP finishes its sync cycle.

If the synchronization fails, there is a retry interval of 60 minutes. The WSUS Synchronization Manager component will schedule the sync to run again 60 minutes after the process fails, and start all over. WSUS Synchronization Manager will create a status message 6703 in the case of a sync failure.

When an SMS 2003 site is upgraded, supported software updates are migrated into the Configuration Manager database and marked as Expired. Before Configuration Manager clients are able to scan for update compliance and before software update deployments can be created, those updates must be put back into an active state by running a sync cycle.

SMS 2003 clients that are on a Configuration Manager site will use the Inventory Tool for Microsoft Update (ITMU) to scan for updates that are in the Microsoft Update catalog. This catalog must be synced for the SMS 2003 clients to be able to scan for the latest updates. By default, the ITMU tool will update the catalog every 7 days using the ITMU advertisement that was set up when it was installed on the SMS 2003 central site.

Compliance

When software update synchronization completes at each site, a site-wide machine policy is created that allows client computers to retrieve the location of the WSUS server and to start a scan for software update compliance. When a client receives that machine policy, a compliance assessment scan is scheduled to start at a random time within the next two hours. When the scan runs, a component of the Software Updates Client Agent clears the previous scan history, sends a request to find the WSUS server that should be used for the scan, and then updates the local Group Policy with the WSUS server location.

The scan request is then passed to the Windows Update Agent (WUA). The WUA then connects to the WSUS server that it just got information about and downloads a list of the software updates that have been synced with the WSUS server, and scans the client computer for the updates in the list. A component of the Software Updates Client Agent then sees that the scan for compliance is finished and sends a state message for each software update that had a change in compliance state since the last scan. Those state messages are then sent to the client's management point in bulk every five minutes. The management point will then forward the state messages to the site server, where they are inserted into the site server database.

Supersedence is when a new software update has the same fixes as a previous update but may have fixed issues with the update and/or have added new fixes. In SMS 2003, when new software updates supersede ones that had the same fixes, they may both be marked as needed when only the new one was necessary. In Configuration Manager 2007, Software Updates now uses the Windows Update Agent (WUA) and partially fixes this problem. When new software updates are released that supersede others, Microsoft Update is refreshed with that information. When client computers are scanned for compliance, the new updates produce a compliance state by the client, but the older updates do not. The only time this is not the case is when a service pack contains a required update. The WUA will then return a compliance state on both, which allows admins to deploy individual updates or service packs as needed. Table 7.7 show details on the four states of compliance for Software Updates.

Deployment

The compliance assessment data is then used to determine which software updates are required on client computers. When you create a software update deployment with the Deploy Software Updates Wizard, as described later in this chapter, the software updates in the deployment are downloaded from the location specified on the Download Location page of the wizard to the configured package source, if they haven't been downloaded already. When the wizard finishes, a deployment policy is added to the machine policy for the site. The updates are then copied from the package source to the shared folders on the distribution points (DP) set up in the package, where they will be available for clients.

When a client in the target collection of the deployment receives the machine policy, the software update client component starts an evaluation scan. Updates that are still required on the client are then added to a class in Windows Management Instrumentation (WMI). Any updates that are mandatory deployments are downloaded as soon as possible from the DP to the local cache on the client. The updates in the optional deployment category are not downloaded until they are manually started. If an optional deployment has a deadline that makes it mandatory, the client will download the update as soon as it registers the change in deployment status.

TA	BLE 7.7:	Software Updates Compliance State	
	STATE	DESCRIPTION	
	Required	The software update is applicable to the client, which means any of the following conditions could be true:	
		◆ The update has not been deployed to the client.	
		The update has been installed, but the state of the update hasn't been updated in the database yet.	
		The update has been installed but the client requires a reboot before it finishes.	
		◆ The update has been deployed but is not yet installed.	
	Not required	The update isn't applicable on the client. The update is applicable on the client and it has already been installed. This state usually means that the software update has been synced to the site server, but the client hasn't been scanned for compliance for that update.	
	Installed		
	Unknown		

SOFTWARE UPDATES IN CONFIGURATION MANAGER ARE ALWAYS DOWNLOADED TO THE CLIENT

Software Updates are always downloaded to the local client cache before they are run in Configuration Manager. You no longer have the option to have them run from a distribution point as you did in SMS 2003.

If the client can't find the location of the DP through Location Services, it will keep trying for up to five days before it stops. If the client can't connect to the DP to download the updates, it will try for up to 10 days before it stops trying. When you start updates manually, the client will try every hour for each DP for up to four hours before it fails.

When an update deployment has a deadline that becomes available on a client, the Available Software Update icon will show up in the notification area to tell a user that the deadline is coming up. By default, these display notifications will show up on a periodic basis until all mandatory updates have been installed. They will be displayed every three hours for deadlines more than 24 hours away, every hour for deadlines less than 24 hours away, and every 15 minutes for deadlines less than an hour away.

Just imagine the phone calls if you left things that way! Fortunately, Microsoft has given you the option to turn that off with a site-wide setting that lets you hide all software update deployments from users. This setting doesn't affect regular Software Distribution settings, but it will keep display notifications, notification area icons, and software update installation progress boxes from showing up at all. However, this will also mean that you can only send out mandatory software update deployments to your clients. We recommend doing that anyway because users would more than likely delay deployments until they were mandatory in the first place.

Unless you hide your update deployments, users will be able to open the Express/Advanced dialog box to start up the installation of all mandatory software updates at once. They will also

be able to open the Available Software Updates dialog box, and then they can choose to install whatever is available.

When the deadline passes on a mandatory update, a scan will start on the client to make sure that the update is still required; the local client cache will be checked to make sure the update is still available and then begin installing the update. When that is done, another scan starts to make sure that the update is no longer required on the client. Finally, a state message is sent to the management point saying that the update is now installed.

Planning to Use Software Updates in Configuration Manager

Now that you have seen what is new in Configuration Manager Software Updates, the prerequisites, and the major components of the process, you can learn the steps necessary to plan the use of Software Updates in your environment.

To plan the implementation of the new version of Software Updates in Configuration Manager, you can use the same process of deployment intelligence that we used to plan the deployment of Configuration Manager itself in Chapter 2. Using this method will help you ensure that you get everything out of Software Updates that your company requires to keep your computer resources up-to-date with the latest software upgrades and patches.

Deployment intelligence for Software Updates has three parts:

- ◆ Determine what needs to be accomplished with Software Updates.
- Determine what is on the network now and what has been used in the past.
- Test in an isolated lab.

Determine What Needs to Be Accomplished with Software Updates

This may seem like a no-brainer, as the first thing that probably comes to mind is "deploy patches." This might have been fine with software updates in SMS 2003, but with Configuration Manager you can do a lot more than just deploy security patches, as we will learn in this chapter.

This part of the planning will also enable you to decide how you want to configure your test environment, your Software Update Point (SUP) infrastructure, and the settings for the Software Update Servers and Client agent settings.

PLANNING FOR SOFTWARE UPDATE POINT INFRASTRUCTURE

The central site server is the primary site server at the top of the Configuration Manager hierarchy. An active SUP is configured on the central site so that software updates can be managed. Most of the synchronization settings are configured there and propagated down to the rest of the sites in the hierarchy. The active SUP on the central site is what syncs with Microsoft Update.

All primary sites in Configuration Manager must have an active SUP. The child sites sync with the active SUP that is set up on its parent site. Secondary sites can be set up with an active SUP, or clients at the secondary site can connect directly to the active SUP on the parent primary.

When your site is in native mode, there is the option to have the active SUP configured to accept connections from both clients on the intranet and the Internet or from only clients on the intranet. When Internet-based client connectivity is not accepted on the active SUP, you can set up separate active Internet-based SUPs if needed.

This site system server role must be assigned to a site system server that is remote from the site server and the active SUP. When the active Internet-based SUP doesn't have connectivity to the

active SUP for the site, you will have to use the export and import functions of the WSUSUtil tool to sync the software update metadata.

If you are going to have more than 25,000 clients connecting to WSUS on the active SUP, a Network Load Balancing (NLB) cluster must be configured on the WSUS server and then configured for the Configuration Manager site so that the NLB cluster is used as the active SUP.

PLANNING FOR THE SOFTWARE UPDATE POINT INSTALL

Before setting up the active SUP site system role in Configuration Manager, there are several requirements that must be considered depending on your Configuration Manager infrastructure, such as when the Configuration Manager active SUP will be configured to communicate using SSL, or when the site server is in native mode, and so on. Additional steps must be taken before the SUP in the hierarchy will work properly.

As discussed earlier in the chapter, Software Updates requires that Windows Server Update Services (WSUS) 3.0 SP1 is installed on all site systems servers that will be configured for the Software Update Point site system role. There can be many site systems with the SUP role, but only one site system can be configured as the active SUP. Also, when the active SUP is not on the site server itself, the WSUS 3.0 Administration console is required on the site server, which lets the site server communicate with the WSUS components on the active SUP. If you are going to use an NLB cluster, the full install of WSUS 3.0 is required on all site systems that will be in the cluster.

During the WSUS install, you can choose to use the default or a custom web site to host the WSUS components. If WSUS is going to be installed on a primary Configuration Manager site system, Microsoft recommends that you choose a custom web site so that IIS hosts the WSUS 3.0 services in a dedicated website instead of sharing the site with Configuration Manager site systems or other applications.

You can use a WSUS server that was active in your environment before Configuration Manager was implemented. When the WSUS server is configured as the active SUP the sync settings are then specified. All of the software updates metadata from the WSUS server will be synced to the Configuration Manager database regardless of the sync settings for the active SUP.

When your Configuration Manager site server is in native mode or when the active SUP point is configured to use SSL, a web server signing certificate must be assigned to the website used by WSUS. When you use a custom website for WSUS, per Microsoft's recommendation, the WSUS website must be assigned a web server certificate where the Subject Name or Subject Alternate Name contains the Internet fully qualified domain name (FQDN). The upstream WSUS server must be set with the same certificate or SSL communication will fail between the servers. The certificate must also reside in Trusted Root Certification Authorities in the Computer certificate store on each client computer, or they will fail to scan for software update compliance.

When the site server is in native mode, the web server certificate that is used for the Configuration Manager site systems can also be used by the WSUS website. Also, when the WSUS uses the same website as the Configuration Manager site server, and the site is in native mode, the default website might already be assigned the right web server certificate. The certificate would still need to be configured on the upstream WSUS server, but it should already be configured on Configuration Manager clients.

If there is a firewall between the Configuration Manager active SUP and the Internet, an active SUP and its upstream server, or an active Internet-based SUP and the active SUP for the site, the firewall might have to be configured to accept the HTTP and HTTPs ports used for the WSUS website. By default, a WSUS server that is configured for the default website uses port 80 for HTTP and 443 for HTTPS communication, while one configured for a custom website uses port 8530 for HTTP and 8531 for HTTPS communication.

If your company doesn't allow these ports and protocols to be open for all addresses on the firewall between the active SUP and the Internet, you can restrict access to the following URIs so that WSUS and Automatic Updates can communicate with Microsoft Update.

```
http://windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com
https://*.windowsupdate.microsoft.com
http://*.update.microsoft.com
https://*.update.microsoft.com
http://*.windowsupdate.com
http://download.windowsupdate.com
http://download.microsoft.com
http://*.download.windowsupdate.com
http://*.download.windowsupdate.com
http://*.download.windowsupdate.com
http://test.stats.update.microsoft.com
http://test.stats.update.microsoft.com
```

If there is an active Internet-based SUP, or there are child sites with an active SUP, these addresses might also need to be added to a firewall that is between the servers:

```
http://<FQDN for active software update point on child site> https://<FQDN for active software update point on child site> http://<FQDN for active software update point on parent site> https://<FQDN for active software update point on parent site>
```

PLANNING THE SOFTWARE UPDATES SERVER SETTINGS

There are software update point settings and general site settings that have an impact on software updates in Configuration Manager. These settings configure the active SUP, and determine what updates are synchronized, whether there are maintenance windows for installing updates, how much time software updates have to complete, and so on.

The SUP settings configure which site system server is the active SUP, which site system server is the active Internet-based SUP if one is specified at the site, the sync source, the sync schedule, the products, classifications, and languages for which software updates will be synchronized.

General Settings

These settings in the New Site Role Wizard and the Software Update point properties set whether the active SUP is a local server or a remote server, and if it uses an NLB cluster. They also set which port settings are used for connectivity to the site system server that is assigned the SUP role, whether a Software Update Point connection account should be used instead of the computer account, if Internet-based clients are allowed to connect the SUP when the site is in native mode, and if SSL is used when synchronizing data from the active SUP and when clients connect to the WSUS server on the active SUP.

Internet-Based Settings

When the Configuration Manager site server is in native mode and the active SUP is configured with Do Not Allow Access From Internet-based clients, an SUP site system role must be created (but not configured as the active SUP) and then configured to be the active Internet-based SUP from the Internet-Based tab in the Software Update Point Component Properties box. You can then set if the active Internet-based SUP is a remote server or uses an NLB cluster, which port settings are used for connectivity to the SUP server, and so on. If synchronization is not configured, the export/import function for the WSUSUtil tool will have to be used to sync update metadata.

Synchronization Settings

The sync settings for the active SUP specify the sync source and whether WSUS reporting events are created during the sync process.

Synchronization Source The sync source for the active SUP at the central site is configured to use Microsoft Updates. The active SUP on child sites is automatically configured to use the active SUP on its parent site as the sync source. When there is an active Internet-based SUP, the active SUP for the site is automatically set to be the sync source. Also, the active SUP or active Internet-based SUP can be configured not to sync with the configured sync source and you can use the export and import function of the WSUSUtil tool instead.

WSUS Reporting Events The Windows Update Agent (WUA) on clients can create event messages that are used for WSUS reporting. These events are not used in Configuration Manager, so the Do Not Create WSUS Reporting Events setting is selected by default. When these events are not created, the only time clients should connect to the WSUS server is during software update evaluation and compliance scans. If these events are needed outside of the Configuration Manager reporting for software updates for some reason, then you will need to modify this setting for your specific needs.

Synchronization Schedule The sync schedule can be configured only at the active SUP on the central Configuration Manager site. When this schedule is configured, the active SUP on the central site will start syncing with Microsoft Update at the scheduled date and time. The custom schedule allows you to sync software updates on a date and time when the demands from the WSUS server, site server, and the network are low, and less likely to interfere with regular network traffic. You can also run a sync cycle manually from the central site from the Update Repository using the Run Synchronization action in the Configuration Manager console.

After the active SUP successfully syncs with Microsoft Update, a sync request is sent to the active Internet-based SUP, if there is one, and to the active SUP on child sites. This process repeats throughout the hierarchy until it is successful.

Update Classifications

Updates are defined with classifications that help to organize the different types of updates. During the sync process, the software updates metadata for the specified classification that will be synchronized. Table 7.8 shows the classifications of updates that can be synced with Configuration Manager.

You will need to decide if you are going to deploy some or all of these categories, or even pick and choose specific updates from each category, in your environment. The update classification settings are configured only on the active SUP highest in the Configuration Manager hierarchy. They are not configured anywhere else because they synchronize the metadata from the upstream sync source using the class settings from the central site. When you choose update classes to sync, remember that the more classes you choose, the longer it will take to sync the software updates metadata.

Products

The metadata for each update sets the product or products for which the update is applicable. A product is a specific edition of an operating system (such as Windows XP) or application, while a product family is the base operating system or application to which the individual products belong (such as Microsoft Windows). You can choose a product family or individual products within a product family.

TABLE 7.8:	Update Classes
-------------------	----------------

UPDATE CLASS	DESCRIPTION
Critical Updates	Broadly released fixes for specific problems addressing bugs that are critical but not security-related.
Definition updates	Updates to virus or other definition files.
Drivers	Software components designed to support new hardware.
Security Updates	Broadly released fixes for specific products, addressing security issues.
Service Packs	Cumulative sets of all hotfixes, security updates, and updates created since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features.
Tools	Utilities of features that aid in accomplishing a task or set of tasks.
Update rollups	Cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a specific component such as IIS.
Updates	Broadly released fixes for specific problems addressing non-critical, non-security-related bugs.

When updates are applicable to several products and at least one of the products is one you have chosen to update, all of the products will appear in the Configuration Manager console even if they haven't been selected.

The product settings, like other software update settings, are configured only on the active SUP highest in the Configuration Manager hierarchy.

Languages

This setting allows you to configure the languages for which the summary details will be synced for a software update and the update file languages that will be downloaded for the software update.

Update File

The languages configured for the update file setting provide the default set of languages that will be available when downloading updates at the site server. When on the Language Selection page of the Deploy Software Updates Wizard or Download Software Updates Wizard, the languages configured for the active SUP are automatically selected, but they can be modified each time updates are downloaded or deployed. When the wizard finishes, the software update files for the configured languages are downloaded, if they are available, to the deployment package source location and copied to the distribution points configured for the package.

The update file language settings should be configured with the languages that are most often used in your environment. For example, if your clients use English and Spanish for the operating systems or applications, and not much else, then select those languages in the Update File column and clear the others. This will allow you to use the default settings on the Languages Selection page

of the wizards most of the time, and also keeps unneeded update files from being downloaded. This setting is configured at each SUP in the Configuration Manager hierarchy.

Summary Details

During the sync process, the summary details info (software updates metadata) is updated for the updates in the languages selected. The metadata provides information about the software update, such as name, description, products supported; update class, article ID, download URL, applicability rules, and so on.

When selecting the summary details languages, you should select only the languages needed in your environment. The more languages that are selected, the longer it will take to sync the software updates metadata. The metadata is displayed in the locale of the operating system where the Configuration Manager console is running. If localized properties for the software are not available, the information displays in English.

Maintenance Windows

Maintenance windows provide admins with a way to define a period of time that limits when changes can be made on the systems that are members of a collection. Maintenance windows restrict when the software updates in deployments can be installed on client computers, as well as operating system and software distribution advertisements.

Client computers determine whether there is enough time to start a software update install by using the following settings:

Restart Countdown The length of the client restart notification (in minutes) for computers in the site. The default setting is 5 minutes, and is a global site setting that can be changed in the Computer Client Agent Properties dialog box.

System Restart Turnaround Time The length of time given for computers to restart and reload the operating system. This setting is in the site control file and has a default of 10 minutes.

Maximum Run Time The amount of time that is estimated for a software update to install on a client. The default is 20 minutes for updates, and 60 minutes for a service pack. This time frame can be changed for each software update on the Maximum Run Time tab for the properties of a software update.

When these setting are used to determine the available time in a maintenance window, each software update has a default of 35 minutes. For service packs, the default is 75 minutes. When you plan for maintenance windows in your deployments, take these defaults into consideration. When planning software update deployments, be aware of the collections Maintenance Window, and how many updates are in a deployment, so you can calculate whether clients will be able to install all the updates within the maintenance window or the installation of updates will span multiple maintenance windows.

When a software update installation completes but there is not enough time left in the maintenance widow for a restart, the computer will wait until the next maintenance widow and restart before starting any more update installs.

If more than one update is to be installed on a client during a maintenance window, the update with the lowest maximum run time installs first, then next lowest installs, and so on. Before installing each update, the client will verify that the available maintenance window is long enough to install the update. After an update starts installing, it will continue to install even if the install goes beyond the end of the maintenance window.

When you create a software update deployment, there are two settings that can allow maintenance windows to be ignored.

Allow System Restart Outside of Maintenance Widows

This option will set whether you want to allow system restarts for both workstations and servers outside of configured maintenance windows. By default, this setting is disabled. This setting comes in handy when you want your software update install to complete on clients as soon as possible. When this setting is not enabled, a system restart will not be triggered if the maintenance window ends in 10 minutes or less. This could prevent the install from completing and leave the client in a vulnerable state until the next maintenance window. This setting is available on the Restart Settings page of the Deployment Template Wizard or the Deploy Software Updates Wizard.

Ignore Maintenance Windows and Install Immediately at Deadline

This setting determines whether software updates in the deployment are installed at the deadline regardless of a configured maintenance window. It is disabled by default and is only available when there is a deadline set up for a deployment. This setting comes in handy when there are software updates that must be installed on clients as soon as possible, such as security patches to fix a vulnerability that is being exploited on the Internet. This setting is available on the Schedule page of the Deploy Software Updates Wizard.

Software Update Properties

Each Software Update has a properties box with three tabs that provide configuration settings to enable software updates and configure the update settings on clients.

Maximum Run Time Tab This tab allows you to set the maximum amount of time a software update has to complete installing on clients, in minutes. If the maximum run-time value has been reached, a status messages is created and the deployment is no longer monitored. This setting is also used to determine whether the update should be started within a configured maintenance window. If the maximum run-time value is greater than the time left in the maintenance window, software update installation is not initiated until the start of the next maintenance window. Keep in mind that if a maximum run-time value is set for more time than the configured maintenance window of a collection it targets, it will never run on those clients. This setting can be configured only on the site synchronized with Microsoft Update, which is more than likely the central site, and the default is 60 minutes for service packs and 20 minutes for all other types. Values can range from 5 to 9999 minutes.

NAP Evaluation Tab This tab is used to set whether the software update is required for compliance when using Network Access Protection (NAP). Enable NAP evaluation to include the software update in a NAP policy that will become effective on NAP-capable clients based on the configured schedule. When the policy becomes effective, NAP-capable clients might have restricted network access until they comply with the selected software update. Network restriction and remediation depend on how the policies are configured on the Windows Network Policy server. Chapter 14 describes how to set up Network Access Protection.

Custom Severity Tab This is a nice addition to Software Updates that allows you to assign custom severity values for software updates if the default value doesn't meet your organization's needs. The custom values are listed in the Custom Severity column in the Configuration Manager console. The software updates can be sorted by custom severity values, the search

folder can be created based on these values, queries and reports can be made that filter on these values — whatever suits your needs. This setting can only be configured on the site that syncs with Microsoft Update.

PLANNING FOR SOFTWARE UPDATE CLIENT SETTINGS

The software updates client settings in Configuration Manager are site-wide and are configured with some default settings at installation. There are Software Updates Client Agent settings and general settings that affect when updates are scanned for compliance, and how and when updates are installed on clients. The client agent settings specific to software updates are configured in the Software Updates Client Agent properties, and the site-wide general settings related to software updates are configured within the Computer Client Agent properties. The software updates installation schedule can be modified from the Configuration Manager icon in the Control Panel on the client. There are also Group Policy settings on the client computer that might need to be configured depending on your environment.

COMPUTER CLIENT AGENT SETTINGS

The properties for this client agent are found on four tabs that provide configuration settings that affect the software update reminders and the customization for software update deployments on clients.

General Tab

On the General tab you can specify a polling interval and a reporting cycle for state messages.

Interval The Policy Polling Interval (Minutes) setting sets how often clients retrieve the machine policy. This setting is relevant to software updates in that when new deployments are created, the machine policy is updated with the deployment information. Clients can take up to the policy polling interval to get those changes, depending on when they last got policy. By default this is set for 60 minutes.

State Messages The State Message Reporting Cycle (Minutes) setting specifies how often clients send state messages to the management point. The software updates client creates state messages for scan, software updates compliance, deployment evaluation, and deployment enforcement. The default setting for this is 5 minutes.

Customization Tab

On this tab you can provide custom information about the update that will appear on clients.

Organization Name The setting specifies the name of the organization authoring the software update install. By default this text box displays "IT Organization." The organization name appears in software updates display notifications, the Available Software Updates dialog box, and the restart countdown dialog box on clients that are deployed software updates. Microsoft recommends that you customize this with something related to your organization.

Software Updates This setting sets an optional subheading used by software updates dialog boxes on clients. By default, the text box displays "Protecting your computer." The Software Updates setting appears in the Available Software Updates and restart countdown dialog on clients that get software update deployments.

Reminders Tab

The settings on this tab specify how often notifications are displayed on client computers when a deployment deadline is approaching for software updates. The reminder intervals can be configured for when the deadline is greater than 24 hours, when the deadline is less than 24 hours away, and when the deadline is less than an hour away.

BITS Tab

The settings on this tab specify if bandwidth throttling is configured for the site. These settings apply to Configuration Manager clients when they use BITS to download software update files from distribution points.

Restart Tab

These settings configure the start countdown timeframe and restart final notification when a software update is installed on client computers, and they use BITS to download software update files from distribution points. By default, the initial countdown is 5 minutes and a final notification is displayed when there is 1 minute before the restart will be started.

CLIENT CONFIGURATION MANAGER PROPERTIES

The Configuration Manager Properties box in the Control Panel of a Configuration Manager client provides software update actions and configuration settings.

Actions

The following actions are applicable to software updates:

Software Updates Deployment Evaluation Cycle When this action is started, active deployments will be evaluated.

Software Updates Scan Cycle Starts a software updates software scan when run.

Updates Tab

This setting configures whether there is a schedule for installing software updates that are required on the client computer. When this setting is disabled, mandatory software updates will be installed at the deadline date and time scheduled by the Configuration Manager admin or manually installed prior to the deadline. When this setting is enabled, it allows you to schedule software update installs at a time that is convenient, such as every day at 2 a.m. If there are several users using a computer, the setting that was configured last is used.

Install Required Updates on a Schedule

This setting determines whether a required software update that has been deployed to this client will install on a specific schedule. When this setting is enabled, you can set a recurrence pattern of every day, or a specific day of the week, and a specific time. Local users and administrators can modify this setting.

GROUP POLICY SETTINGS

These settings in Group Policy are required for the Windows Update Agent (WUA) on client computers to connect to WSUS on the active software updates point and successfully scan for software update compliance.

Specify Intranet Microsoft Update Service Location

When the active SUP is created for a site, clients receive a machine policy that provides the active SUP server name and configures the "Specify intranet Microsoft update server location" local policy on the computer. The WUA retrieves the server name set with "Set the intranet update service for detecting updates," and then connects to that server when it scans for software updates compliance. When a domain policy has been created for the "Specify intranet Microsoft update service location" setting, it will override local policy, and the WUA might connect to a server other than the active SUP. If that happens, the client computer might scan for software update compliance based on different products, classes, and languages. Microsoft recommends that this domain policy not be configured for Configuration Manager clients.

Allow Signed Content from Intranet Microsoft Update Service Location

Before the WUA on clients will scan for updates that were created and published with the System Center Updates Publisher, the "Allow signed content from intranet Microsoft update service location" Group Policy setting must be enabled. When the policy setting is enabled, the WUA will accept updates received through an Internet location if the updates are signed in the Trusted Publishers certificate store on the local computer.

Configure Automatic Updates

The Automatic Updates feature allows clients to receive security update and other important downloads. It is configured through the Configure Automatic Updates Group Policy setting or the Control Panel on the local computer. When Automatic Updates is enabled, clients will receive update notifications (if you have notifications enabled) and download and install required updates. When Automatic Updates coexists with software updates, each might display notification icons and popup display notifications for the same update. Also, when a restart is required, each might display a Restart dialog box for the same reason.

Self Update

During a Configuration Manager client install, the Windows Update Agent (WUA) is installed on a client computer if it is not already installed. When Automatic Updates is enabled, the WUA on each client automatically does a self update when a newer version becomes available or when there are problems with the component. When Automatic Updates are not configured or are disabled, the WUA is still installed during Configuration Manager client installs. If the WUA install fails becomes corrupt, or there is a new version of WUA available, a software distribution must be created to update the agent on clients. If the WUA fails on a client, the scan for software update compliance also fails until it is fixed.

Determine What Is on the Network Now and What Has Been Used in the Past

If you are upgrading from SMS 2003, there are special considerations for your current system of software updates. Some of the scanning tools that SMS uses will no longer work; others will only work with SMS 2003 clients. If you are using other tools for software updates, you will have to determine how they figure in to Configuration Manager's software update infrastructure.

PLANNING FOR THE SMS 2003 SOFTWARE UPDATES UPGRADE

There are several things to consider when planning for software updates after upgrading from SMS 2003 to Configuration Manager. This section gives information about what software update

info is upgraded and about scanning computers for software updates compliance, software updates metadata, software updates synchronization, deploying software updates, and using software updates reporting.

The site server upgrade from SMS 2003 to Configuration Manager updates the SMS 2003 files and the SQL Server database. The details on the upgrade are logged in <code>%systemdrive%\ConfigMgrSetup.log</code>. The following software updates information is migrated from the SMS 2003 schema to the Configuration Manager schema:

- Existing SMS 2003 software update distributions will be migrated and continue to work as expected only when the advertisement and program are created at the site that is being upgraded. Software update installation programs created at the site being upgraded will not be migrated if the advertisement was created at a child site. The programs that aren't migrated will continue to work on SMS 2003 clients, but Configuration Manager clients will not retrieve the updates deployed using these install programs.
- Information about the installed version of the Inventory Tool for Microsoft Updates. Other
 inventory scan tools are not compatible with Configuration Manager, and information
 about these tools will not be migrated.
- ◆ Software updates metadata, such as the name, description, applicability rules, article ID, the URL for more information about the update, the bulletin ID, the path to the software update source files, associated products, and other details. Until software updates are synchronized, all updates will be put in an expired state. Before you upgrade, make sure that you still have a valid package source for each package. If the package source is not valid, you will have to download all of the content in the package source again or the validation check will fail and the content will be invalidated.
- ◆ Compliance information for the software updates, such as the number of scanned clients in which the software update is required or not.
- Client status information, such as the revision of the Microsoft Update catalog that is used when clients scan for update compliance.
- Security rights for SMS 2003 objects that were migrated to Configuration Manager.

SCANNING FOR SOFTWARE UPDATE COMPLIANCE AFTER A SITE UPGRADE

There are several inventory scan tools in SMS 2003 that scan client computer for software update compliance. When you upgrade to Configuration Manager, Inventory Tool for Microsoft Updates (ITMU) is fully operational on all client computers, the Inventory Tool for Custom Updates (ITCU) is supported, but with certain conditions, and the other scan tools have very limited support.

Inventory Tool for Microsoft Updates

During the SMS 2003 upgrade to Configuration Manager, Setup will detect if a previous version of the ITMU is installed. Setup assumes that the ITMU is installed in the highest site in the hierarchy and that the tool is not installed on any other sites. When the ITMU tool is found, Setup will start a silent upgrade for the inventory tool on the site server. After the ITMU has been upgraded, the catalog will be synced with the latest Microsoft Updates catalog, the new scan package will be updated, and clients will upgrade the scan tool during their next Machine Policy Retrieval & Evaluation Cycle. The client will then scan for update compliance using the Microsoft Update catalog. Only SMS 2003 clients should be in the target collection for the Microsoft Update Tool

advertisement, as it is not supported on Configuration Manager clients. When all of your SMS 2003 clients have been upgraded to Configuration Manager, then the ITMU tool should then be uninstalled from the site server.

Inventory Tool for Custom Updates

After a site upgrade, SMS 2003 clients in the hierarchy will continue to scan custom software updates for compliance using the scan package for the ITCU. For Configuration Manager clients to scan for custom software updates, the custom catalog must be republished to the update server using the System Center Updates Publisher, and then the SUP must be synced with the published updates.

Other Inventory Scan Tools

After a site upgrade, scanning for update compliance using all other inventory scan tool catalogs is only supported for SMS 2003 clients left in the hierarchy, and is not supported for Configuration Manager clients.

Synchronizing Software Updates after a Site Upgrade

As discussed earlier, during a site server upgrade all software updates are migrated in the Configuration Manager database and the Expired attribute for each update is then set to Yes. Before Configuration Manager clients are able to scan for software update compliance and before software update deployments can be created at the site server, the updates must be put back into an active state by running a software update sync cycle.

Synchronizing the Microsoft Updates Catalog

After the ITMU tool is upgraded, the Microsoft Updates catalog is automatically synced using the Microsoft Updates Tool Sync advertisement. When it's complete (which may take over an hour), the synchronized software updates from the Microsoft Updates catalog are reset to an active state.

Synchronizing the Software Update Point

After a site upgrade, the Software Update Point role must be created and configured and then synchronized with the WSUS server. This process is detailed later in the chapter.

Software updates from only the Microsoft Updates and custom software updates catalogs can be synced with the site server database. All other updates will remain in an expired state, will not be scanned for compliance on clients, can't be deployed to client computers, and will eventually be removed.

Deploying Updates to Clients

After the Configuration Manager upgrade, advertisements that were active prior to the upgrade will continue working on SMS 2003 clients. These advertisements are moved to the SMS 2003 Advertisements node under Software Updates\Deployment Management in the Configuration Manager console. New deployments can be made to SMS 2003 clients after the SUP is created, configured, and synchronized with the WSUS server.

The Deploy Software Updates Wizard is used to deploy software updates to both Configuration Manager and SMS 2003 clients. Only software updates from Microsoft Update and published custom updates can be deployed to SMS 2003 clients, and catalogs from other scan tools are not supported.

Using Deployment Templates That Specify SMS 2003 Settings

When deployment templates are created with the Deploy Software Updates To SMS 2003 Clients setting enabled, the template will be available on the Deployment Template page of the Deploy Software Updates Wizard only when all updates can be deployed to SMS 2003 clients.

USING THE SOFTWARE UPDATE REPORTS

The software update reports and the SQL views that provide them with data have been modified to work with the new software update system in Configuration Manager. The SMS 2003 reports are migrated during the Configuration Manager upgrade, but because the new software update reports are based on state messages forwarded from clients instead of hardware inventory, they might not work or provide the right data. Several new reports have been provided to report on software updates in Configuration Manager, and they are grouped in the following categories:

- Software Updates A. Compliance
- Software Updates B. Deployment Management
- Software Updates C. Deployment Status
- Software Updates D. Scan
- Software Updates E. Troubleshooting
- Software Updates F. Distribution Status

Test in an Isolated Lab

It is important to understand how software updates will work in your environment, and one way you can do that is to set up a test lab that is as close to your production environment as possible. This section describes a minimum setup of Configuration Manager to use while you are testing or evaluating the software update components.

To start, you will need at least one computer for each operating system that you use in your environment. Also, you will need computers that have other crucial line-of-business applications running on them, as well.

A single client is adequate for minimum test purposes, but if you want to have a representative sample of how software updates will work with all computers used in your enterprise, then you will need to have a representative of each client configuration in your environment. For example, if you are using Windows XP SP2, Windows Server 2003 R2 SP2, and Windows Vista Business in your organization, then you should have at least one client with each of those operating systems on it for testing. If you plan on later migrating to Windows Server 2008, you should have a computer with the latest version of that OS on it as well. If you can't get that many machines together, at least try to get one beefed up computer with lots of RAM. That way, you can use Virtual Server or Virtual PC to set up virtual representations of the computers that you couldn't manage to procure physically.

By doing this, you will become familiar with how the Software Updates components and the actual software update executables work with the operating systems on your network before you use Software Updates enterprise-wide. By using more than one operating system in your testing you will be able to:

 Review the specific software updates that Microsoft has published for those operating systems

- Start becoming familiar with software update management practices for each type of computer
- Learn how software updates work with different operating systems in a controlled environment
- Learn how to find information about specific software updates for a specific OS when you need it

REQUIREMENTS FOR TESTING SOFTWARE UPDATE POINTS

When you test software updates, create the SUP site role as it would be in your production site. You will need to decide if a single active SUP will be created or if there will be an active SUP for connectivity from client computers on the Internet, and if the active SUP will be set up with an NLG cluster. The deployment intelligence that you have gathered up to this point will be crucial to helping you plan your test environment.

REQUIREMENTS FOR TESTING FOR A MIXED HIERARCHY

If you have SMS 2003 sites in production, you should have at least two in the test hierarchy, with SMS 2003 clients like the others you already have set up, and software updates working on them. You can then upgrade the test SMS 2003 central site in order to monitor and become familiar with the upgrade procedures and the post-upgrade configuration that will be needed. Once that is done and you have configured the upgraded site for software updates, you can run test deployments targeting both Configuration Manager and SMS 2003 clients. This will allow you to become familiar with the Configuration Manager objects, as well as the special SMS 2003 objects that get created.

TESTING NETWORK ACCESS PROTECTION

This may be a little more difficult to test as NAP in Configuration Manager works in conjunction with policies on a Windows Server 2008 computer running Network Policy Server to enforce compliance with selected software updates. For more information on this, see Chapter 14.

Configuring Software Updates

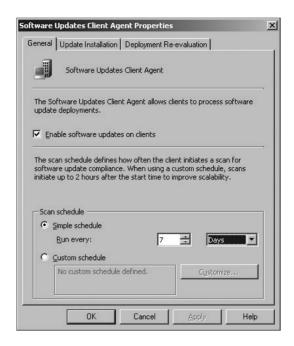
Now that we have taken time to look at the parts of Software Updates and how they fit together, and you have taken that information with your deployment intelligence and worked together a plan on how you want to set up Software Updates in your environment, we can examine how to get everything working.

Before Software Updates data can be displayed in the Configuration Manager 2007 console, and software updates can be deployed to clients, the SUP must be set up and configured, as well as the rest of the components of Software Updates.

Configuring the Software Updates Client Agent

The Software Updates Client Agent is enabled in Configuration Manager by default, but you still have to configure the other settings of this client agent to match your plans for using Software Updates in your environment.

FIGURE 7.1 The Properties ➤ General tab of the Software Updates Client Agent



To configure the Software Updates Client Agent, follow these steps:

- **1.** In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ [site code] ➤ [site name] ➤ Site Settings ➤ Client Agents.
- 2. Right-click on Software Updates Client Agent, and then click Properties.
- **3.** On the General tab (shown in Figure 7.1), you can configure the following settings.

Enable Software Updates on Clients

This setting defines whether the Software Updates Client Agent is enabled for the site; this agent is installed and enabled on Configuration Manager clients by default. Make sure that this setting is enabled. If the client agent is disabled, the client agent components are put into a dormant state but not uninstalled, and existing deployment policies will be removed from clients as well. Re-enabling the client agent starts a policy request that the components on clients be enabled and the deployment metadata be downloaded. The Software Updates Client Agent is configured on a site-by-site basis and affects only clients assigned to that site. If you want to have the Software Updates Client Agent configuration the same across your Configuration Manager hierarchy, you can use Transfer Site Settings to deploy those settings across your hierarchy.

Scan Schedule

This setting specifies how often the client computer scans for software updates compliance. By default, a simple schedule is configured to run the scan every 7 days and the site database is updated with any changes since the last scan. The minimum value for the scan is 1 minute and the maximum value is 31 days. This setting can be set only

after an active Software Update Point site role has been installed on a site system in the site. When a custom schedule is configured, the actual start time on client computers is the start time plus a random amount of time up to 2 hours. This keeps the clients from starting a scan and connecting to WSUS all at the same time.

4. Click the Update Installation tab, and then configure these settings:

Enforce All Mandatory Deployments

This sets whether to enforce all mandatory software update deployments that have deadlines within a certain time frame. When a deadline is reached for a mandatory software update deployment, an installation is started on the clients that have been targeted for the mandatory deployment. It also sets whether to start the install for updates defined in other mandatory deployments that have a configured deadline within a specified time frame. The benefits of this setting are that it expedites software update installs for mandatory updates and that it might increase security, decrease display notifications, and decrease system restarts on clients. This setting is disabled by default.

For Deployments Deadlines Within

This sets the time frame for the Enforce All Mandatory Deployments setting. The minimum value allowed is 1 to 23 hours, and 1 to 365 days. By default, this setting is configured for 7 days.

Hide All Deployments from End Users

We highly recommended this setting, unless your company requires it otherwise. With this setting enabled, all deployments are hidden when they are received on client computers. Use this setting to deploy updates to computers without any display notifications or notification area icons. This setting is disabled by default.

- 5. Click the Deployment Re-Evaluation tab to configure how often the Software Updates Client Agent reevaluates software updates for installation status. When software updates that have been installed are no longer found on client computers and are still required, they will be reinstalled. This reevaluation schedule will need to be adjusted based on company policy for update compliance, whether users have the ability to uninstall updates, and similar considerations. You also have to consider that every reevaluation cycle results in some network and client computer activity. The minimum value allowed for the deployment revaluation schedule is 1 day and the maximum is 31 days. A simple schedule of every 7 days is set by default.
- **6.** When you have finished setting things the way you want, click OK to finish.

Installing Windows Server Update Services 3.0 Server

Windows Server Update Services 3.0 Server (WSUS) SP1 is required in order to use Software Updates in Configuration Manager 2007. Installing WSUS for use with Configuration Manager is different from a standard install of WSUS without the Configuration Manager infrastructure.

The WSUS installation procedure that we are about to outline can be used for both active SUPs (the main Software Update Point installed on the central site) and inactive SUPs (those for any other primary Configuration Manager sites), or for installing WSUS on a remote server that is not a Configuration Manager site server. Installing WSUS on the same server as your site servers, or on another remote server, will depend on your server resources and your plan for the software update infrastructure.

After that, you have to go through a series of steps to make a Software Update Point the active one for the Configuration Manager hierarchy. We will detail those steps later on in the chapter.

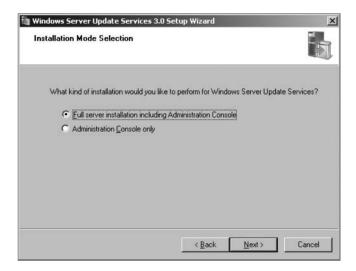
If you haven't already done so, make sure that you have downloaded the latest version of WSUS at the WSUS home page:

http://www.microsoft.com/downloads/details.aspx?familyid=F87B4C5E-4161-48AF -9FF8-A96993C688DF&displaylang=en

To install WSUS, perform the following steps:

- Double-click the WSUS install file that you downloaded, WSUSSetup_30SP1_x86.exe (or WSUSSetup_30SP1_x64.exe for the 64-bit version of Windows Server 2003), and you will see the opening page of the Windows Server Update Server 3.0 Setup Wizard.
- 2. Click Next, and then select Full Server Installation Including Administration Console, as is shown in Figure 7.2, and click Next again.

FIGURE 7.2
Installation Mode
Selection



- 3. Click the I Accept The Terms Of The License Agreement check box, and then click Next.
- **4.** The next screen, shown in Figure 7.3, will ask you to choose if you want updates to be stored on the WSUS server.
 - So that you can accept Software License Terms that might be required by some updates, you must select the default option and keep a copy of these updates locally. Choose where you want to keep these files and then click Next.
- 5. The next page, shown in Figure 7.4, lets you choose your database options. If you are not installing WSUS on a Configuration Manager site, the default of Install Windows Internal Database On This Computer is probably your best option, as it installs Microsoft SQL Server 2005 Embedded Edition just for the purpose of managing WSUS. This will save you from having to purchase another full SQL Server license for WSUS, and managing another instance of SQL as well.
 - If you are installing WSUS on a Configuration Manager primary site server and it has the resources to handle it, then we recommend going ahead and using the instance of

SQL Server 2005 that is already installed. (If it doesn't have the resources, you probably shouldn't be installing WSUS on this server anyway.) Having two versions of SQL installed on the same server could cause problems in the long run, and they would be competing for the same resources.

Depending on what you choose, WSUS will either create the Windows Internal Database or test the connection to the existing SQL Server instance. After that is done, click Next.

FIGURE 7.3Selecting an update source page

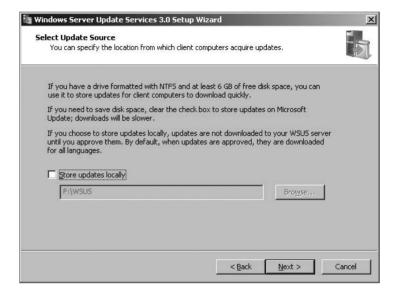
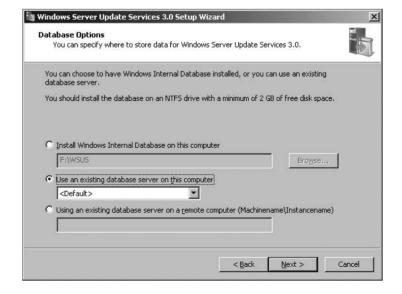


FIGURE 7.4
The Database Options
page of the Windows
Server Update Services
3.0 Setup Wizard



6. The next page of the wizard, shown in Figure 7.5, lets you choose how to configure the WSUS website.

Microsoft recommends that you choose to make a custom website if you are using WSUS as a SUP, even if the WSUS server is remote from the Configuration Manager site system. You should definitely use the custom site option if you are installing WSUS on a Configuration Manager site, so that the install will not interfere with the other Configuration Manager components that use IIS. By default, the custom WSUS website uses HTTP port 8530 and HTTPS 8531. Click Next.

FIGURE 7.5
The Web Site Selection page of the wizard



7. After that, review the settings and click Next. When the wizard is done, click Finish. The WSUS configuration wizard will start up after that, but you should close it, as Configuration Manager will take care of configuring all of the settings for WSUS.

Installing the Windows Server Update Services 3.0 Administration Console

The Windows Server Update Services (WSUS) 3.0 SP1 administrator console is required on the Configuration Manager 2007 site server, if WSUS is installed on a remote server, to allow it to communicate to with WSUS so it can configure and synchronize SUPs. The WSUS administration console can be installed using the WSUS 3.0 Setup Wizard, or installed silently from a command line.

To install the WSUS on a Configuration Manager site server, follow one of the procedures discussed in the sections that follow.

INSTALL WSUS ADMINISTRATOR CONSOLE USING THE SETUP WIZARD

Take the following steps to install the administrator console using the wizard:

- 1. Double-click the WSUSSetup_30SP1_x86.exe setup file that you downloaded earlier.
- **2.** Click Next to get past the first page of the wizard, and then select Administrator Console Only, as shown in Figure 7.6. Click Next again.

- 3. Click "I accept the terms of the License Agreement" and click Next.
- **4.** If you see the Required Components To Use Administration UI page, shown in Figure 7.7, click Next.
 - The Microsoft Report Viewer 2005 redistributable will have to be installed, as it is required to open the WSUS console. It isn't needed when you are using WSUS with Configuration Manager, however.
- 5. When the wizard is done, click Finish.
- **6.** To verify that the install completed, click Start ➤ All Programs ➤ Administrative Tools, and then click on Microsoft Windows Server Update Services 3.0. To verify that connectivity, connect to the WSUS server that you are going to use with Configuration Manager.

FIGURE 7.6
The Installation Mode
Selection page of the
Windows Services
Update Server 3.0 Setup
Wizard

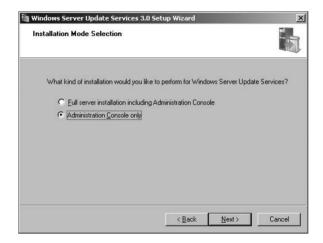


FIGURE 7.7
The Required Components to Use Administration UI page of the Windows Services
Update Server 3.0 Setup
Wizard



INSTALL THE WSUS 3.0 ADMINISTRATION CONSOLE FROM THE COMMAND PROMPT

Take the following steps to install the administration console using the command line:

- In the folder where you have already downloaded the WSUS installer file, open up a command prompt.
- **2.** In the command prompt window, type the following command:

```
WSUS3Setupx86.exe /g CONSOLE INSTALL=1
```

The WSUS 3.0 Administration console will then install silently.

3. Verify the install as in Step 6 of the previous procedure.

Setting Up the Active Software Update Point

There can be several Configuration Manager site systems with the Software Update Point system role, but there can be only one site system sever configured as the *active* SUP (the one configured to get updates from Microsoft Update) in a Configuration Manager site. When your Configuration Manager site is in native mode, you can have an active Internet-based SUP assigned to a remote site system server that allows communication from only Internet-based client computers. Also, if the active SUP is on a Network Load Balancing (NLB) cluster, there should be an SUP installed on every server that is in the NLB cluster.

To set up an active SUP, follow these steps.

- **1.** In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ [site code] ➤ [site name] ➤ Site Settings ➤ Site Systems.
- **2.** Decide whether to create a new site system server or add the Software Update Point role to an existing site system. Depending on which you choose, take the next step:

New Site System with Software Update Point

Right-click Site Systems, click New, and then choose Server.

Add the Software Update Point Role to an Existing Server

Right-click the site system you want to use, and then click New Roles.

3. What you do next will depend on your site settings. By default, the computer account for the site server will connect to the site system computer (if installing on a separate site) and install the necessary components. If the computer account of the site server has access to the site system server and the Configuration Manager site is in mixed mode, the settings shown in Figure 7.8 are optional. In the following screen shots, we are adding the Software Update Point Role to our central Configuration Manager server.

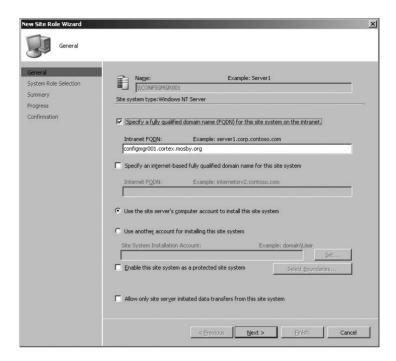
When the computer account does not have access to the site system server or when the site.

When the computer account does not have access to the site system server or when the site is in native mode, you will have to configure the following settings on the New Site Role page:

Specify a fully qualified domain name (FQDN) for this site system on the intranet

You will have to configure this setting for an active SUP when the site server is in native mode or when it is in mixed mode and using Secure Sockets Layer (SSL). By default, you must configure this setting.

FIGURE 7.8
The General page of the New Site Role
Wizard page



Specify an Internet-based fully qualified domain name for this site system

You must configure this setting if you are setting up an active SUP that accepts Internet-based client connections, or for the active Internet-based SUP.

Use another account for installing this site system

This setting is configured when the computer account for the site server doesn't have access to the remote site system being set up as an SUP.

Allow only site server initiated data transfers from this site system

This setting must be used when the remote SUP doesn't have access to the inboxes on the site server. This will let a site system from a different domain or forest put files that need to be transferred to the site server. The site server will connect to the remote site system and get the files every so often. The Internet-based SUP might need this setting to be enabled to work.

After you have configured what you need to, click Next.

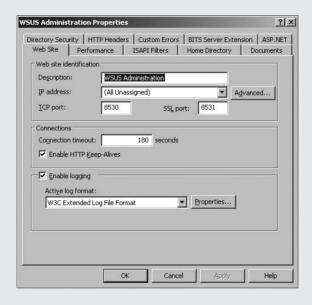
- 4. Select Software Update Point from the list of available site roles, and then click Next.
- **5.** If you are going to be using a proxy server to connect to the SUP, enter those settings and click Next. Otherwise, just click Next.
- **6.** In the Active Software Update Point Settings page (see Figure 7.9), choose whether the SUP you are setting up will be the active SUP for your site, and specify the port settings that are used by the WSUS you are connecting to.

By default, the port settings for a WSUS custom website (the recommended setting) are HTTP port 8530, and HTTPS port 8531. If you installed WSUS on the Default website, the ports are HTTP port 80 and HTTPS port 443.

FINDING THE PORTS USED BY WINDOWS SERVER UPDATE SERVICES

If someone else installed the WSUS server that is being used for an SUP, you may not know what ports were used during setup. If you input the wrong ports on this page of the wizard, the setup will fail. You can find the ports used by WSUS by following these steps:

- 1. Under Administrative Tools, click on Internet Information Services (IIS).
- 2. Expand Web Sites, right-click the website that is being used for WSUS, and click Properties. A custom WSUS site is recommended, but the Default website might have been used as well.
- 3. Click the Web Site tab, shown here. The HTTP setting is displayed in the TCP Port field, and the HTTPS port setting is in the SSL Port field.



7. Choose the synchronization source for the active SUP by selecting one of the options shown in Figure 7.10:

Synchronize from Microsoft Update

The SUP that is highest in the Configuration Manager hierarchy (usually the central site) must use this setting.

Synchronize from an Upstream Update Server

The active SUP on all child sites and on all Internet-based SUPs should use this setting. The wizard will select this option as the default if the SUP meets the criteria.

Do Not Synchronize from Microsoft Update or an Upstream Update Server

Use this setting when the active SUP can't connect to the upstream update server. This will usually be used by an active Internet-based SUP that doesn't have access to the active SUP. The active SUP on the central site can't use this setting. Synchronizing an SUP through importing and exporting updates is covered later in the chapter.

8. On that same page, accept the default of Do Not Create WSUS Reporting Events, and then click Next.

FIGURE 7.9
The Active Software
Update Point Settings
page of the New Site
Role Wizard

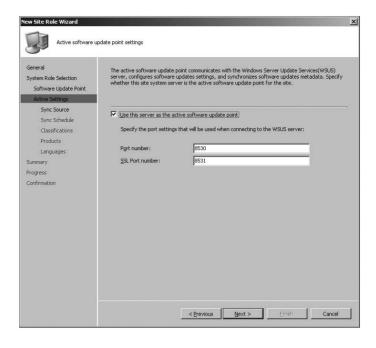
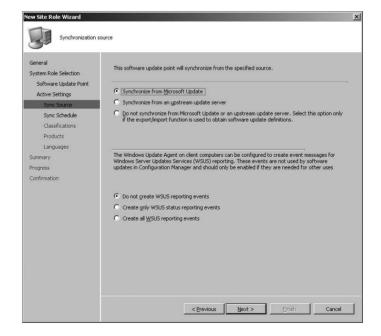
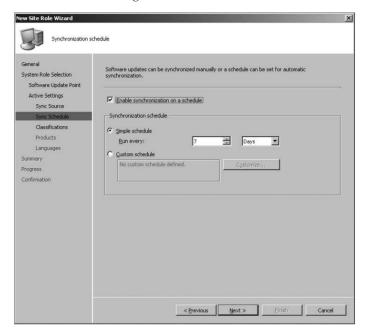


FIGURE 7.10
The Synchronization
Source page of the New
Site Role Wizard



9. Choose whether to synchronize software updates on a schedule, by selecting Enable Synchronization On A Schedule, as shown in Figure 7.11.

FIGURE 7.11 Synchronization page



This is disabled by default, and you can start a manual sync by running the Run Synchronization action in the Configuration Manager console. We recommend that you enable a schedule, as scheduled syncs perform full synchronizations, and manual syncs will only do delta synchronizations of software updates. Once you have made your choice, click Next.

- **10.** Choose the update classifications that you want to deploy with software updates, and then click Next. The Classifications page is shown in Figure 7.12.
- 11. Choose the products that you want to deploy, as shown in Figure 7.13, and then click Next.
- **12.** Select all the languages that you will be supporting with software updates, as shown in Figure 7.14, and then click Next. Click Next again on the following page, and click Close.
- **13.** To monitor the install of the SUP, open up the SUSSetup.log in the *<Configuration Manager Install Path>*\Logs folder. When the install is finished, you will see the text Installation was successful.
- **14.** Open the WCM. log in the same directory to verify that the connection to the WSUS server worked. When the connection to the WSUS server is made and the WSUS components are checked, you will see

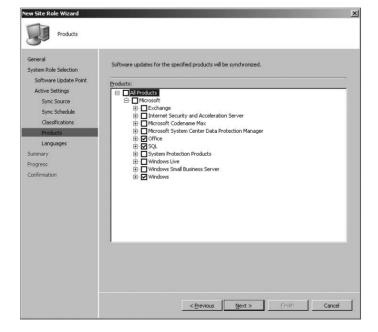
There are no unhealthy WSUS Server components on WSUS Server servername and

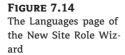
Successfully checked database connection on WSUS server *servername* in the log file.

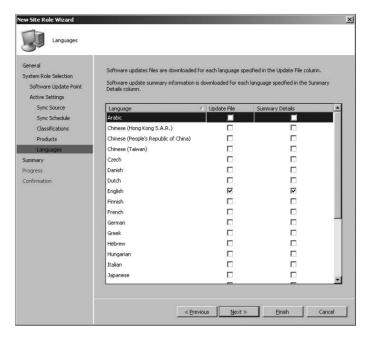
FIGURE 7.12
The Classifications page of the New Site Role
Wizard



FIGURE 7.13
The Products page of the New Site Role Wizard







In this procedure, the only difference between making an active SUP and a nonactive SUP is not checking the Use This Server As The Active Software Update Server setting in Step 6. If you don't select that option, that is where you finish the wizard. Otherwise, everything else is the same as described, depending on what kind of SUP you are trying to setup.

Configuring Software Updates Settings and Synchronization

Software updates in Configuration Manager 2007 must be synchronized with Microsoft Update before information on those updates will be available to view in the Configuration Manager console. Synchronization starts at the highest level in the hierarchy that has an active SUP and either has a configured schedule or is started manually using the Run Synchronization action.

When synchronization is started on a configured schedule, all changes to the Software Updates metadata since the last scheduled sync are inserted into the site database. This will include metadata for new software updates or metadata that has been modified or deleted. When a sync is started manually, only new Software Updates data since the last sync is inserted into the database. The manual sync process is faster since it is not pulling as much Software Updates metadata. A manual sync action is only available on parent sites.

The synchronization process might take longer than an hour to finish, depending on several factors, including whether a synchronization has been run before and what languages, products, and update classifications have been configured to be synchronized. You can monitor the synchronization process by looking at the log file for WSUS synchronization manager, wsyncmgr.log. This is located by default at

%Program Files%/Microsoft Configuration Manager/Logs

When the synchronization is complete, you will see a 6702 status message from SMS_W-SUS_SYNC_MANAGER.

When the synchronization with Microsoft Update is complete (either from a schedule or started manually) at the highest site in the hierarchy, sync requests are sent to all child sites and they in

turn start synchronization with their configured upstream WSUS servers as soon as the request is finished processing.

The Software Updates metadata that is synced from Microsoft Update is based on the update classes, products, and languages that were selected when the active SUP was first configured. A child site will synchronize whatever updates have been configured on its parent site.

Although all of the settings for update classes, products, and so on were configured at the setup of the SUP, you can still reconfigure these options if needed. To configure the update properties for software updates, follow these steps.

- In the Configuration Manager console for the highest site in the hierarchy with software updates enabled, go to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ [site code] ➤ [site name] ➤ Site Settings ➤ Component Configuration.
- 2. Right-click Software Update Component, and then click Properties.
- **3.** To configure Update Classifications, click the Classifications tab, as in Figure 7.15.
- **4.** To configure products that are being synced, click the Products tab, shown in Figure 7.16.
- **5.** To configure languages that are being synced, click the Languages tab shown in Figure 7.17.

FIGURE 7.15Software Updates: Classifications tab

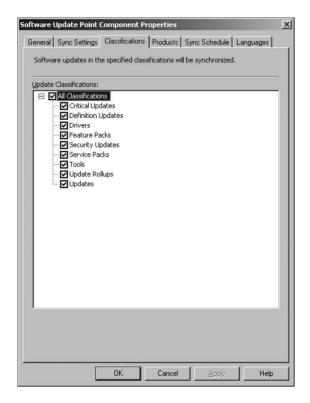


FIGURE 7.16Software Updates: Products tab

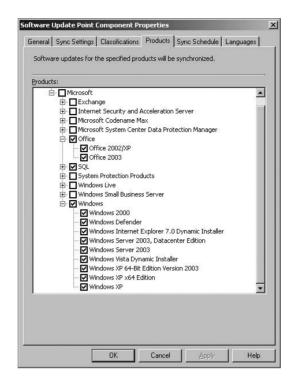
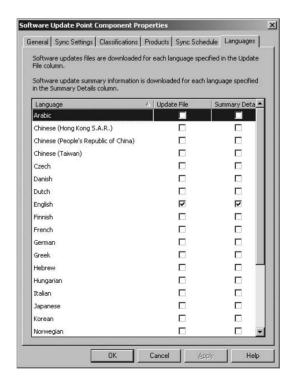


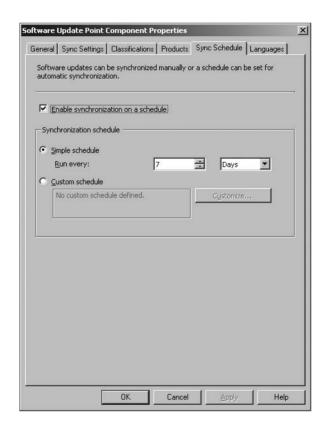
FIGURE 7.17 Software Updates: Languages tab



To configure the software updates synchronization schedule, follow these steps:

- In the Configuration Manager console for the highest site in the hierarchy with software updates enabled, go to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ [site code] ➤ [site name] ➤ Site Settings ➤ Component Configuration.
- 2. Right-click on Software Update Component, and then click Properties.
- **3.** To configure the synchronization schedule, click on the Sync Schedule tab, shown in Figure 7.18.

FIGURE 7.18
Software Updates: Sync
Schedule tab



- **4.** To enable synchronization on a schedule, select Enable Synchronization On A Schedule and set the schedule as you want it.
- 5. When you are done, click OK to save the schedule. Unless you change the Start value in the custom schedule, synchronization will be started as soon as possible and will repeat based on the schedule that you configured.

To start a sync cycle manually, follow these steps:

 In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Updates ➤ Update Repository. 2. Right-click on Update Repository and then click Run Synchronization. A sync will be started as soon as possible, and a request to sync child sites will be sent out as soon as it is complete.

Synchronizing Updates with Export and Import

When an SUP is not configured or cannot synchronize with its upstream server in the Configuration Manager 2007 hierarchy, the export and import function of the WSUSUTIL tool can be used to synchronize Software Updates metadata manually. The user who performs the export/import must be a member of the local Administrators group on the WSUS server, and the tool must be run locally on the WSUS server itself.

The files found in the WSUSContent folder (by default located in <WSUSInstallDrive> \WSUS\WSUSContent) must also be copied from the upstream update server to the SUP so that locally stored updates and the license terms for the updates are available to the import server.

To export and import software updates from the export WSUS server to the import WSUS server, follow these steps:

- **1.** Copy files from the export server to the import server:
 - a. On the export server, go to the folder where software updates and the license terms for those software updates are stored. By default, this will be <WSUSInstallDrive> \WSUS\WSUSContent.
 - **b.** Copy all of these files to the same folder on the import server.
- **2.** Export metadata from the database of the export server:
 - a. At a command prompt on the export WSUS server, go to the folder that contains WSUSUtil.exe. By default, this will be located at "ProgramFiles"\Update Service\Tools.
 - **b.** Then type the following:

```
WSUSUTIL.exe export packagename logfile
```

The name of *packagename* doesn't really matter, as long as it and the log file are unique in that folder. This command will export the software updates metadata into a file called *packagename*.cab.

- c. Move the export package that you just made to the folder that contains WSUSUtil.exe on the import WSUS server.
- **3.** Import metadata to the database of the import server:
 - **a.** At a command prompt on WSUS server that you are importing the updates to, go to the folder that contains WSUSUtil.exe, which is *%Program Files*%\Update Services\Tools.
 - **b.** Type this command:

```
WSUSUTIL.exe import packagename logfile
```

with *packagename* being the name of the export file that you exported in step 2. This will import all the metadata from the exporting server and create a log file that you can use to review the status.

Supporting Software Updates for SMS 2003 Clients

The Inventory Tool for Microsoft Updates (ITMU) that is used by SMS 2003 clients is automatically upgraded when an SMS 2003 site is upgraded to Configuration Manager. This tool is also on the Configuration Manager install DVD if it needs to be installed later.

After an SMS 2003 site is installed or upgraded, the updated inventory tool downloads the Microsoft Updates catalog from the download section, synchronizes the software updates in the catalog, and then stores that information in the site database. When the inventory tool is run on client computers, it will scan for software update compliance based on that catalog.

Before you deploy this tool to your SMS 2003 clients, you should do a test deployment on the test client that you chose during the ITMU install, to make sure all the processes are running. This tool is not supported on Configuration Manager clients.

INSTALLING THE INVENTORY TOOL FOR MICROSOFT UPDATES (ITMU)

If the ITMU install becomes corrupt, or you add a site to the Configuration Manager hierarchy that has SMS 2003 clients that you have to support, there might be a need to install the ITMU on your Configuration Manager site. To install the ITMU tool on the highest site in your Configuration Manager site hierarchy, follow these steps:

- Find the ITMU install file, SMSITMU.msi, located on the Configuration Manager install DVD in \DVD Drive\SMSSETUP\SUMSCANTOOLS\1386.
- **2.** Run the install file on the central Configuration Manager site server; this will launch the ITMU Setup Wizard. On the Welcome screen, click Next.
- 3. Select I Accept The License Agreement as shown in Figure 7.19, and then click Next.

FIGURE 7.19
The License Agreement screen

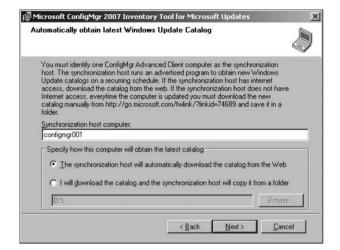


- **4.** Install the ITMU tool in the default location or somewhere else that you want, as shown in Figure 7.20, and click Next.
- **5.** Type in a Configuration Manager client as the synchronization host, as shown in Figure 7.21. This client will get the updated catalog on a schedule that you will configure later.

FIGURE 7.20Selecting a destination folder



FIGURE 7.21
Automatically obtain
the latest Windows
Update catalog

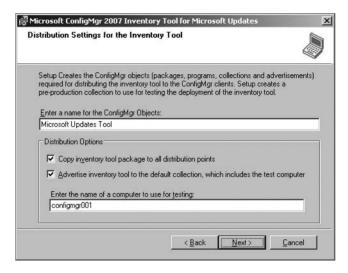


You can make this the central site for faster processing of data because whatever you choose will need a fast connection to the site server database.

- **6.** On that same page, choose from the following two options.
 - ♦ If the site server has Internet access, select The Synchronization Host Will Automatically Download The Catalog From The Web, and the site server will connect to Microsoft Updates to download the update catalog.
 - ◆ If the site server doesn't have Internet access, select I Will Download The Catalog And The Synchronization Host Will Copy It From A Folder to get the catalog from the location you enter in the input field. You will have to download the catalog from another computer and then put it in the folder you enter here. The URL that is listed on this page is the place to get the catalog file. Once you have filled out the proper information, click Next.

7. The Distribution Settings For Inventory Tool page, as shown in Figure 7.22, lets you set the names of the objects created by the ITMU install.

FIGURE 7.22
Distribution Settings for the Inventory Tool



These objects will include everything that is needed to distribute the tool to SMS 2003 clients: packages, programs, collections, and advertisements that will be created by the install program. Choose a new name and enter it here, or leave the default name that is provided. Whatever you choose, do not change it after the install is complete or the ITMU tool may not work properly.

On this same page, in the Distribution Options section, you have three more options:

- ◆ Decide whether the ITMU package will be sent to all distribution points in the site hierarchy. This is enabled by default, and if it is disabled, the package will not be copied to any distribution points and you will have to do that manually later.
- Decide whether you want to advertise the inventory tool to the collection that is created during the install, Microsoft Updates Tool (Pre-Production). The test client will be the only member of that collection until you add more manually. This is selected by default.
- Enter the name of the client computer that you want to use for testing the ITMU. The sync host computer is entered by default, but you will want to make sure that this computer is an SMS 2003 client. Once you have made all your decisions, click Next.
- **8.** The Distribution Settings For Windows Update Agent page, shown in Figure 7.23, lets you decide if you want to create objects to deploy the Windows Update Agent to client computers.
 - This is enabled by default, which allows the Windows Update Agent to be installed as a dependent component of the ITMU. You can either keep the default name of the package or change it to another one.





On the same page, you also have more options, under Distribution Options:

- Decide whether you want the Windows Update Agent package to be sent to all the distribution points in the site hierarchy. This option is selected by default, and if you change it the package will not be assigned to any distribution points. You will have to assign distribution points later before you can deploy the package to clients.
- Decide whether to create a package and program for the Windows Update Agent. This will be deployed initially as a dependency of the ITMU, but you will be able to use this later if the agent gets corrupted or downgraded on clients. Once you have made your choices, click Next to go to the Installation page, and click Next to start the install.
- **9.** The Setup Complete page will appear when the install process is finished. It will show information about the install and where you can get further details. Click Finish to close the install and start the synchronization process.

The advertisements, packages, programs, and collections for the Inventory Tool for Microsoft Updates (ITMU) are created as part of the install process. To check to see if the ITMU Objects were installed properly, follow these steps.

- In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Distribution ➤ Advertisements.
- Make sure that the Microsoft Updates Tool and the Microsoft Updates Tool Sync advertisements have been created.
- 3. In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Distribution ➤ Packages.
- **4.** Make sure that the Microsoft Corporation Microsoft Updates Tool 2.0 ALL was created.
- **5.** Expand the package (if it is there) and click Programs. You should see the following programs for that package:

- Microsoft Updates Tool
- Microsoft Updates Tool (expedited)
- Microsoft Updates Tool IA64
- Microsoft Updates Tool IA64 (expedited)
- Microsoft Updates Tool Sync
- Microsoft Updates Tool x64
- Microsoft Updates Tool x64 (expedited)
- **6.** In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Distribution ➤ Collections.
- **7.** Verify that the following collections have been created.
 - Microsoft Updates Tool
 - ◆ Microsoft Updates Tool (pre-production)
 - ◆ Microsoft Updates Tool IA64
 - Microsoft Updates Tool Sync
 - Microsoft Updates Tool x64

To verify that the Microsoft Updates Tool Sync advertisement completed successfully, follow these steps:

- 2. Only one primary site should be listed, so right-click on the name, select Show Messages, and click All to open the Status Message Viewer for that site.
- **3.** Review all the status messages and make sure that the advertisement completed successfully. Exit the viewer when you are done.
- 4. Go to the folder where you installed the Microsoft Updates Inventory Tool (C:\Program Files\Microsoft Updates Inventory Tool) in Windows Explorer, and look in the Pkg-Source subfolder to find the Wsusscan2.cab file. Make sure that it is there and that the file date is recent.
- 5. In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Distribution ➤ Packages.
- Find the package ID for the Microsoft Updates Synch package by looking at the last column for its entry.
- 7. Make sure that the synchronization files are in the package folder on the distribution point by going to
 - <**DP** name>\SMSPKG<driveletter>\$\<packageID> where *package ID* is the ID you got from the last step. Make sure that the inventory scan tool files are there, and close Explorer when you are done.

MONITORING THE SYNCHRONIZATION PROCESS

The synchronization process for the Inventory Tool for Microsoft Updates will start right after the install wizard has completed. To monitor that process, open the wsynchmgr.log file. When the process completes successfully, you will see the status message

6710 - SMS Legacy Update Synchronization Done

appear in the log file. You can also look for this same status message for the SMS_WSUS_SYNC_MANAGER under the Component Status node for the site server.

Preparing Software Updates for Deployment

So far in this chapter, we have planned our implementation of Software Updates, set up and configured Software Updates, and now we are finally ready to deploy software updates to Configuration Manager 2007 clients. Well, nearly ready. We still need to find the updates to be deployed (using any of several methods), download them, and optionally create an update list and/or a deployment template. These tasks can be done in the sequence shown here or independently of each other.

Before we get into that process, there are a few things you should keep in mind after you have set up all of the Software Update components:

1. Give the process a little time to work. Don't expect to set up everything we have discussed so far, and think you are going to be able to do a couple of clicks and deploy updates out to your clients. You are going to have a little bit of lead time as updates are synced with Microsoft Update, the metadata is synced with the rest of the Configuration Manager hierarchy, and clients get requests for scans. Depending on the size of your hierarchy and the number and kind of clients you need to be scanned, this might take a while; after all this is a process.

If you click on the Software Updates node in the Configuration Manager console and don't see any results in your compliance summary, then your clients either haven't been scanned, or they haven't sent their scan results. Until you see something in those reports, you don't have enough to work with to do any update deployments.

With that said, we can continue preparing for software update deployment.

Finding the Software Updates to Be Deployed

Before you can deploy any software updates to clients, you will need to figure out which ones you want or need to deploy to your clients. Configuration Manager provides several ways to do that, and each allows you to find clients that need the updates you want to focus on installed.

When you are looking for updates to deploy, avoid updates that show up in the Configuration Manager console with an icon with a yellow arrow. These are updates that have been superseded by another update that contains the same fixes. To avoid installing outdated components to your clients, do not include these updates in your deployments. They are no longer needed.

There are basically four methods to find needed software updates:

- Software Updates reports
- Software Updates search folders
- The Software Updates home page (in the Configuration Manager console)

The Update Repository node (in the Configuration Manager console)

USING SOFTWARE UPDATE REPORTS TO FIND UPDATES

You can gather compliance information on your clients by running reports under the Software Updates A. Compliance category, as they are designed specifically for this purpose.

To use Web reports from the Configuration Manager console to find required updates, follow these steps.

- In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Reporting ➤ Reports.
- **2.** This will give you a list of all reports in the center pane of the console. Find the report Compliance 5 Updates By Vendor/Month/Year, right-click it, and click Run. The report will display in the center pane as shown in Figure 7.24.

FIGURE 7.24
A sample compliance report displayed in the console

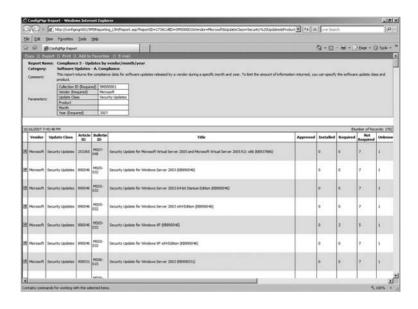


To get an idea of what update data you have collected already, input **SMS00001** for the Collection ID (All Systems), **Microsoft** for the vendor, **Security Updates** for the Update Class, and then the current year in the year value, and click Display. You should see a report like the one shown in Figure 7.25.

Any software updates that meet those criteria will be displayed in the report. The Required column gives the number of clients that require each software update in the list. The report also shows all of the updates that have been deployed by listing an asterisk (*) in the Approved column. To get more information about any of the updates, click on the information link on the far right of the report (you may have to do some side scrolling to see it) and this will pull up the latest information from Microsoft on this update.

3. To get more details click on the drill-down link in the first column of the report, and this will open the Compliance 7 - Specific Software Update States report and you will see a count of computers for each compliance state for that particular update.

FIGURE 7.25 A sample compliance report with values entered for Collection ID, Vendor, Update Class, and Date



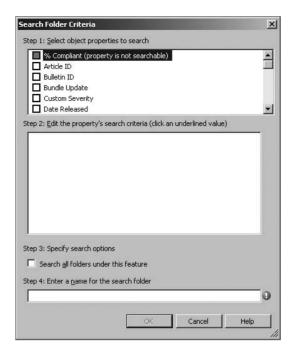
USING SOFTWARE UPDATE SEARCH FOLDERS TO FIND UPDATES

You can create custom search folders with specific criteria that will help you find software updates that are required on client computers. For example, you can make a search folder that displays only Security Updates that have a severity of Critical. Using search folders is part of Microsoft's recommended Software Updates workflow. Taking this further to deploy updates, you can take the search folder of Critical Security Updates mentioned previously, add those into an update list (more on that later), create a deployment using that update list, and then use software reports to monitor the compliance on that update list.

To make a search folder to show software updates, follow these steps:

- In the Configuration Manager console, go to System Center Configuration Manager ➤ Site
 Database ➤ Computer Management ➤ Software Updates ➤ Update Repository ➤ Search
 Folders.
- **2.** Right click on Search Folder and then click New Search Folder. You will then see the Search Folder Criteria dialog box, as shown in Figure 7.26.
- **3.** You want to make a search folder for all critical security updates for Windows 2000. So first you scroll down and look for Severity (for Critical Updates) and click the box next to it. You will see its entry go into the Step 2 window.
- **4.** Look for the Update Classification (for Security Updates) category and select that. You will see its entry go into the Step 2 window as well.
- **5.** Look for the Product (for Windows 2000) category and select that as well, and its entry goes into the Step 2 window.
- **6.** In the Step 2: Edit the Property's Search Criteria window, you'll see three entries for the choices you made on the previous steps. To enter a selection for Product, click the items in To Find that are in blue. When you do, you will see a Search Text window. Scroll through the list and check the box by Windows 2000. Click OK.

FIGURE 7.26 Search Folder Criteria



- By Update Classification, click Items To Find, and check Security Updates in the Search Text window. Click OK.
- **8.** Click Items To Find next to Severity, and select Critical in the Search Text window. Click OK.
- 9. In Step 3: Specify Search Options, select Search All Folders Under This Feature.
- In the Step 4 box, name the search Critical Security Updates for Windows 2000 and click OK
- **11.** Now expand the Search Folders console node and take a look at the search folder that you just made, as displayed in Figure 7.27.

You can find all the updates that need to be deployed to Windows 2000 computers in this search folder by looking at the column labeled Required. You can sort by any column, by clicking on that column. From here you can download these updates, add them to an update list, or deploy them to client computers. Search folders also provide a great way to organize updates before deployment to clients.

USING THE SOFTWARE UPDATE HOME PAGE TO FIND UPDATES

The Software Updates home page lets you find software updates for a specific vendor, during a specific month and year, and for a specific update classification.

To use the Software Update home page to find updates, follow these steps:

In the Configuration Manager console, go to System Center Configuration Manager ➤ Site
Database ➤ Computer Management ➤ Software Updates. You will see the home page,
shown in Figure 7.28.

FIGURE 7.27
The newly created search folder

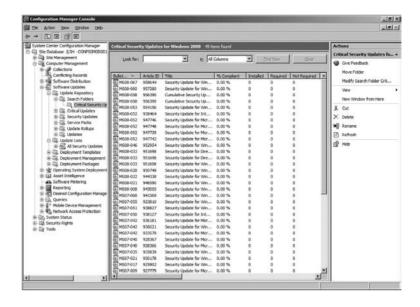


FIGURE 7.28The Software Updates home page



2. The software updates are displayed in the Software Update Compliance Status Summary pane based on the article ID of the update. By default, the software updates from the month when software updates were last synced will be shown. You can change the criteria for this and then click Go to update what is displayed. You can find what software updates are required on clients, and how many need them, by looking at the Required column. Select one or multiple updates in the list, and the pie chart will change to display compliance levels for those updates. From here you can download updates, add them to an update list, or deploy those updates by choosing the appropriate right-click action.

Clicking on the article ID of any of the updates will take you to a Web page with more information on that particular update. Scrolling to the right and clicking on the % Compliant for any of the updates will open up the Compliance 7 - Specific Software Update States report that will show a count of computers in each state of compliance for that update.

USING THE UPDATE REPOSITORY TO FIND SOFTWARE UPDATES

The Update Repository node in the Configuration Manager 2007 console organizes software updates by update classification and then by product. From there you can browse software updates by classification, vendor, or product; or you can create a search folder to find the updates you want to deploy.

To use the Updates Repository node to display software updates, follow these steps:

- In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Updates ➤ Update Repository.
- 2. Choose an update classification and expand it to view it. You can also click on All Updates, and get a list of all updates under that update classification. If you have more than one vendor listed, you can select that vendor to see the list of updates under that classification as well.

Updates are displayed by article ID. You can find what updates are required by clients as you can for other methods, by using the Required column. As in other sections of the console, you can click any column header to sort the data by that column. And as with the other methods, you can download updates, add them to an update list, or deploy them by choosing the appropriate right-click action.

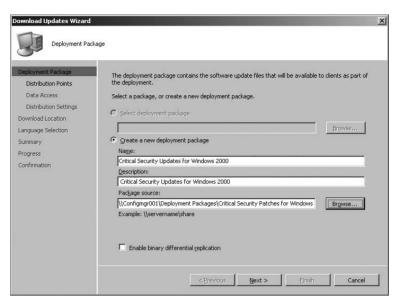
Downloading Software Updates

As you saw in the last section, there are several ways to download software updates in Configuration Manager. The Download Updates Wizard allows you to download selected software updates to a deployment package prior to deploying updates to clients. When you make an update list, the Update List Wizard gives you the option to download the software updates as part of the process of making the list. Finally, the Deploy Software Updates Wizard will download the software updates as part of the deployment process.

Software updates are downloaded from the Internet or from a shared folder on the network that the site server has access to, and that can be added to new or existing deployment packages. To download software updates to a deployment package, follow these steps:

- Go to the software update search folder that you created earlier, by choosing System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Updates ➤ Update Repository ➤ Search Folders ➤ Critical Security Updates for Windows 2000.
- 2. Sort the updates in the list so that the updates required by the most clients are at the top by clicking on the Required column twice.
- Hold down the Shift key and select all the updates that have at least one client requiring that update.
- **4.** Right-click on those updates, and then click Download Software Updates. This will start up the Download Updates Wizard, shown in Figure 7.29.

FIGURE 7.29 The Deployment Package page of the Download Updates Wizard



- 5. If you already have deployment packages created (as described later in the chapter), you can add these updates to one of them in the first field, by selecting Deployment Package. You can click Browse to open up a dialog box that will allow you to select a package that is only for hosting software updates, and select one from the list. Otherwise it will be grayed out as in our example.
- **6.** The other option on this first page of the wizard is to Create A New Deployment Package. There are three fields to fill out, and an option to decide on:

Name

The name of the deployment package. You should pick a unique name that describes the content and is limited to 50 characters or less.

Description

The description of the package that should describe the contents in detail up to 127 characters.

Package Source

The location of the software update source files. You should manually create this share before going any further. When the deployment is created, the source files are compressed and copied to the distribution points that are associated with the deployment package. This location must be entered as a network path (such as \\server\sharename\path) or you can use the Browse button to find the location on the network. This location should not be used by any other deployments or software distribution package.

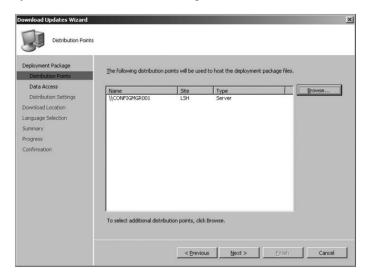
Enable binary differential replication

Allows binary delta comparison to be used on the changed package source files. Checking this box lets Distribution Manager transfer only parts of the files that have changed

instead of the entire file. This saves a lot of bandwidth when copying packages to distribution points.

7. Next is the Distribution Point page, shown in Figure 7.30. The Browse button will allow you to select from the available distribution points on your site that you want use for this software update package. You can leave this blank for now, and the software update files will be downloaded to the source folder. However, the updates will not be available to deploy to clients until you add at least one distribution point.

FIGURE 7.30
The Distribution Point page of the Download Updates Wizard



8. Next is the Data Access Page, shown in Figure 7.31, which appears only if you are making a new deployment package. It has the following options:

Access Distribution Folder Through Common ConfigMgr Package Share

This lets users access the package share through the shared folder for the package (SMSPKGx\$, where x is the drive letter) on a distribution point. This is the default option.

Share Distribution Folder

Lets users access the package through a custom shared folder and path that you create manually prior to choosing this option.

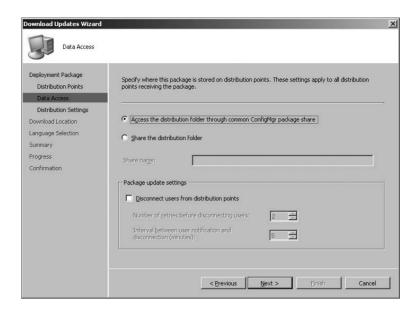
Disconnect Users From Distribution Points

Enables you to determine whether to notify users and disconnect them from distribution points when Configuration Manager updates package data. By default, this setting is disabled. When enabled, you have the following options:

Number of Retries Before Disconnecting Users

The number of times that Configuration Manager tries to update the package source files before starting to disconnect users. The default value is 2 and you can set this to 0 to 99.





User Grace Period (in minutes)

The number of minutes Configuration Manager should wait after notifying users before disconnecting them from distribution points. The default is 5 minutes, but you can set this from 0 to 59 minutes.

9. Next is the Distribution Settings page, shown in Figure 7.32. Its options are as follows:

Sending Priority

The sending priority for the deployment package. The sending priority is used for the deployment package when it is sent to distribution points at child sites. Packages are sent in priority order from High, Medium, or Low. Packages with the same priority are sent in the order they are created. Unless there is a backlog, packages should process immediately no matter their priority. Medium is the default priority.

Preferred Sender

The sender that is used to send this deployment package to other distribution points. By default, this is set to <No Preference>, which lets any sender available be used.

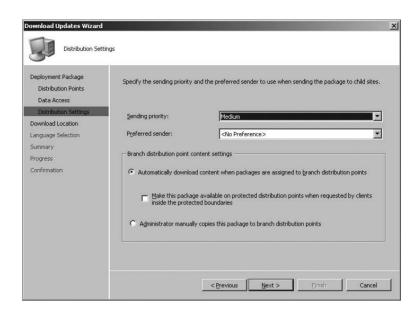
Automatically Download Content When Packages Are Assigned To Branch Distribution Points.

This option is pretty self explanatory.

Make This Package Available On Protected Distribution Points When Requested By Clients Inside The Protected Boundaries.

When a client is within the boundaries of protected distribution points and the client requests the package, then the package is downloaded to the protected distribution points

FIGURE 7.32
The Distribution Settings page of the Download Updates Wizard



Administrator Manually Copies This Package To Distribution Points.

10. Next is the Download Location page, shown in Figure 7.33, with the following options:

Download Software Updates From The Internet

This will download the updates from the location on the Internet that is defined in the software update definition. This is the default setting.

FIGURE 7.33
The Download Location page of the Download Updates Wizard

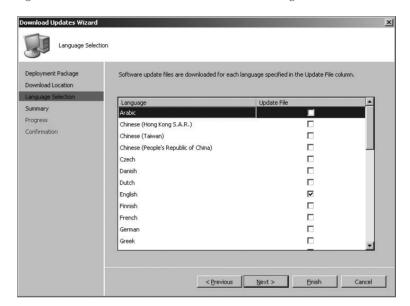
Download Updates Wizard		×
Download Location		
Deployment Package Distribution Points Data Access	If your site server does not have an Internet connection, you can download the software updates from a different computer and save them to a network location accessible by the site server.	
Distribution Settings	Select the download location for software updates:	
Download Location		
Language Selection	© Download software updates from the Internet	
Summary	O Download software updates from a location on the local network	
Progress	Brawse	
Confirmation		
	Note:	
	When the deployment package contains all required software updates, select the "Download software updates from the Internet" option. The software updates files will be validated, but will no be downloaded again.	
	< Previous Next > ⊟nish Cancel	

Download Software Updates From A Location On The Local Network

The software updates are downloaded from a local directory or shared folder that you set in the box. Use this setting when the site server doesn't have Internet access. The software updates can be downloaded from any computer that does have Internet access and stored in a location on the local network that the site server has access to.

11. The Language Selection page (see Figure 7.34) shows the languages in which the software update files will be downloaded. By default, the languages that are configured for the SUP are selected. Adding a selection here does not add it to the SUP settings.

FIGURE 7.34
The Language Selection
page of the Download
Updates Wizard



12. When the wizard is done, the software updates will show up under Deployment Packages ➤ <deployment package name> ➤ Software Updates in the Configuration Manager console.

Creating an Update List

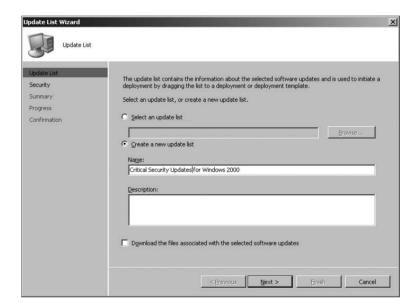
As stated earlier in the chapter, an update list in Configuration Manager contains a set of software updates. An update list offers several benefits when deploying and monitoring software updates and is part of Microsoft's recommended Software Updates workflow. It provides the ability to delegate the administration of approving and deploying software updates. For example, an administrator at the central site can select the software updates that need to be deployed and add the updates to an update list. Administrators at child sites, with restricted rights to objects, can then use the update list and deploy the updates in the update list to the collection that needs them.

Tracking the compliance state for the software updates in deployments is an important task for Configuration Manager admins. When update lists are used, you can use the Compliance 1 - Update List Overall report for the set of updates in the update list, or the Compliance 3 - Update List (Per Update) report to get a list of the updates in an update list and the overall compliance of each. This is a great reason to use the update lists as a part of your software update procedure.

To create an update list, follow these steps:

- Go to the software update search folder that you created in a previous procedure by choosing System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Updates ➤ Update Repository ➤ Search Folders ➤ Critical Security Updates for Windows 2000.
- Sort the updates in the list so that the updates required by the most clients are at the top by clicking on the Required column twice.
- Hold down the Shift key and select all the updates that have at least one client requiring that update.
- **4.** Right-click on those updates, and then click Update List. This will start up the Update List Wizard, shown in Figure 7.35.

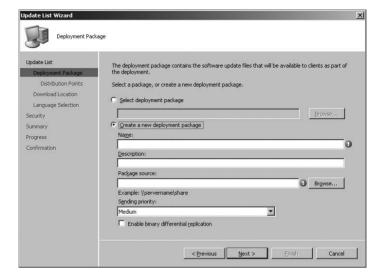
FIGURE 7.35
The Update List Wizard first page



- **5.** Your first option is Select An Update List. If you had already created an update list, you could add the updates you have just selected to a previous list.
- **6.** The second option is to Create A New Update List, which is what you want to do here, so select that option and type in Critical Security Updates for Windows 2000.
- 7. Then you have a description window, where you can type in a description of these updates if you want.
- **8.** The last option is Download The Files Associated With The Selected Software Updates. You have probably already downloaded these in previous procedures, but let's check that option anyway and click Next.

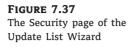
9. This brings you to the Deployment Package page, shown in Figure 7.36. This is almost identical to the Deployment Package page from the Download Updates Wizard. This time you have a deployment package that you want to use, so leave Select Deployment Package selected and click Browse.

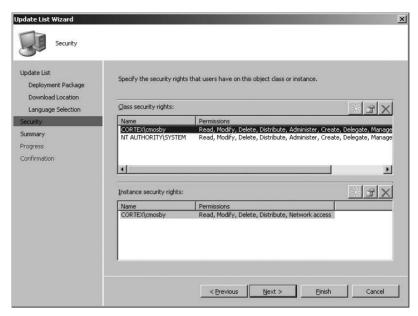
FIGURE 7.36
The Deployment Package page of the Update
List Wizard



- **10.** So far, you have made only one deployment package to choose from, so select Critical Security Updates for Windows 2000 and click OK, and then click Next.
- 11. The Download Location page here is identical to the same page from the Download Updates Wizard shown earlier, in Figure 7.32. You have two choices here either Download Software Updates From The Internet or Download Software Updates From A Location On The Local Network. Choose the first option for our example, and click Next.
- **12.** The Language Selection page appears, which again is the same as in the Download Updates Wizard in the previous procedure (see Figure 7.33). You have nothing to change here, so click Next.
- **13.** You'll see the Security page, shown in Figure 7.37. This is the page that allows you to set permissions for the Update List so you can delegate it to other administrators, just like other Configuration Manager objects. After you set the permission you want, go ahead and click Next.
- **14.** A Summary page now shows all the choices you made. Once you have reviewed that information, click Next and wait for the wizard to let you know it is done. You will see a Confirmation page and you can click Close.

Your new update list will appear in the Update Lists folder under the Update Repository in the Configuration Manager console.





Creating Deployment Templates

As discussed earlier in the chapter, deployment templates can store many of the software update deployment properties. You can create them to maintain consistency, save time, or to fit your software update procedures. By creating deployment templates in advance for typical deployment scenarios in your environment, you'll be able to populate many of the properties that are most often static for the particular deployment scenario. Using the deployment template also reduces the number of wizard pages in the Deploy Software Update Wizard by up to seven pages, depending on what information you have already populated, which saves time and helps to prevent mistakes when setting up a deployment. Templates are created prior to deploying updates by running the Deployment Template Wizard.

To create a deployment template, follow these steps:

- Go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Updates ➤ Deployment Templates.
- 2. The first page of the Deployment Template Wizard is the Template Name page, shown in Figure 7.38. Enter a name for your template in the first field, and a description of the template if you want. Click Next when you are done, which brings up the Collection page.
- **3.** As shown in Figure 7.39, the Collection page has only one field, which lets you choose a collection to receive your deployment. You can leave this field blank if you want to use your template for more than one collection. For our example, we will select All Windows 2000 Professional Systems.

FIGURE 7.38
The Template Name
page of the Deployment
Template Wizard

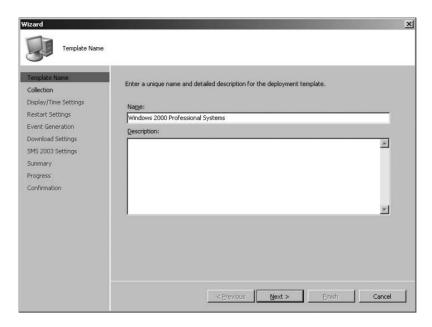
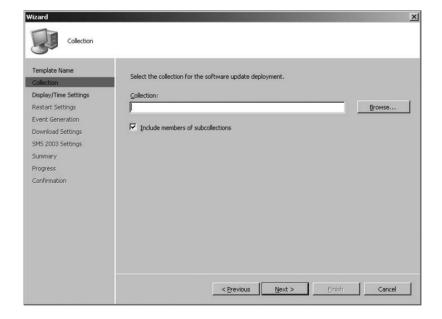
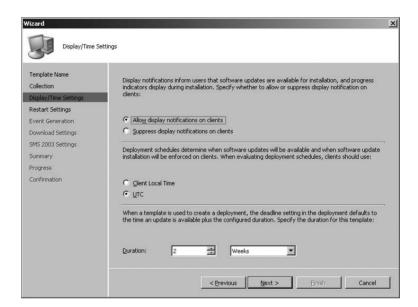


FIGURE 7.39
The Collection page of the Deployment
Template Wizard



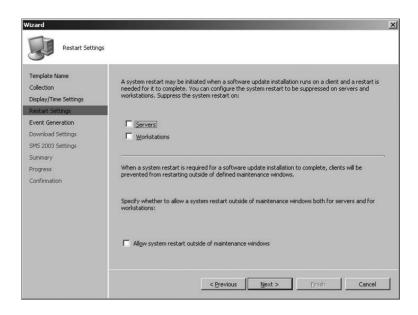
- **4.** The next page is Display/Time Settings shown in Figure 7.40. There are three options on this page:
 - ◆ Allow Display Notifications On Clients or Suppress Display Notifications On Clients (allowing display notifications is the default).
 - Use either Client Local Time or UTC time when evaluating deployment schedules (UTC time is the default).
 - Choose a deadline duration for the template (the default is 2 weeks).
 Global settings for each of these options may override what you choose here.

FIGURE 7.40
The Display/Time Settings page of the Deployment Template Wizard



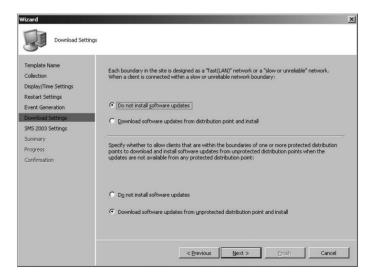
- **5.** The next page is Restart Settings, as shown in Figure 7.41. There are two options to configure on this page:
 - You can choose to suppress reboots on Servers or Workstations, or both by checking each box. If any of the updates that are installed require a reboot, they will be suppressed until either you reboot them manually or another deployment without this option runs and makes them reboot.
 - Choose to allow system restarts outside of any maintenance window schedule.
- **6.** Next is the Event Generation page, which has two options:
 - ◆ Disable Operations Manager alerts while software updates run.
 - ♦ Generate Operations Manager alert when a software update installation fails.

FIGURE 7.41
The Restart Settings
page of the Deployment
Template Wizard



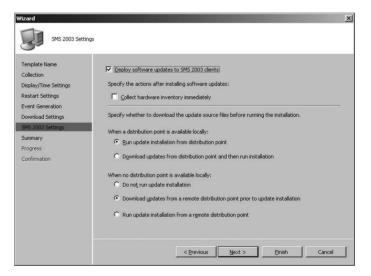
- **7.** Next is the Download Settings page, shown in Figure 7.42. There are two sections on this page:
 - Choose options for clients that are on a "slow or unreliable" network boundary, either Do Not Install Software Update" (the default option) or Download Software Updates From The Distribution Point And Install.

FIGURE 7.42
The Download Settings
page of the Deployment
Template Wizard



- Choose options for clients that are in the boundaries of protected distribution points when updates are not available on protected distribution points, either Do Not Install Software Updates or Download And Install Software Updates From Unprotected Distribution Point And Install (the default option).
- **8.** The next page is for SMS 2003 Settings, as shown in Figure 7.43. This page lets you choose if you want to deploy these updates to SMS 2003 clients, and is disabled by default. If you enable this option, the following settings become available:
 - Specify the actions after installing software updates. Collect Hardware Inventory Immediately is unchecked by default.
 - Specify whether to download the update source files before running the installation.
 When a distribution point is available locally, you have these options:
 - Run update installation from distribution point (default).
 - ◆ Download updates from the distribution point and then run the installation.
 - ♦ When no distribution point is available locally, you have these options:
 - Do not run update installation.
 - Download updates from a remote distribution point prior to update installation (default).
 - Run update installation from a remote distribution point.

FIGURE 7.43
The SMS 2003 Settings page of the Deployment Template Wizard



9. The next page is the Summary page, so you can review the options you selected, and then click Next. Once the wizard is complete, click Close.

When the Deployment Template Wizard is done, the deployment template you made will show up under Deployment Templates. If you need to change things later, you can right-click on your template and choose Properties to change what you need to.

Deploying Software Updates with the Deploy Software Updates Wizard

Now that all the setup and preparation tasks have been done, you are ready to run the deployment. Before deploying software updates, make sure you've considered things like whether the maintenance windows and client restart settings will work for the different clients in your environment, how you are going to handle servers differently than workstations, which deployments will be delegated, and deployments for any leftover SMS 2003 clients.

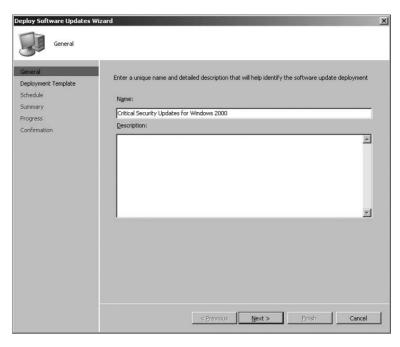
To ensure the most successful software update deployments, utilize update lists and deployment templates that fit the needs of your organization, and keep software updates organized so they are easier to keep track of and deploy. Configuration Manager's software update process is light years ahead of what is part of SMS 2003, so use it to its full potential.

The Deploy Software Updates Wizard in Configuration Manager is what allows you to create or modify software update deployments. Software updates that you want to deploy can be selected from several locations, as discussed earlier in this chapter, and the deployment wizard can be started in different ways as well.

To deploy software updates using the Deploy Software Update Wizard, use the following steps:

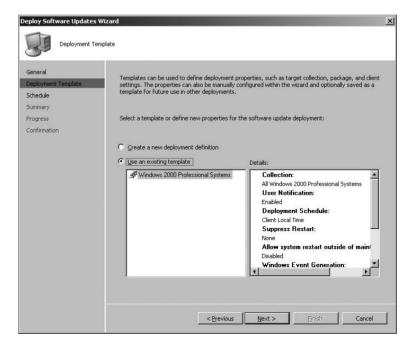
- In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Updates.
- 2. Decide what updates you want to deploy. You can use any of the methods that were described in the Find The Software Updates That You Want To Deploy section earlier in the chapter, or you can just select several updates from any of the Update Repository sections by Ctrl-clicking the updates that you want.
- 3. You can start the Deploy Software Update Wizard using any of the following methods:
 - Right-click some selected updates, or an update list, and then click Deploy Software Updates.
 - Drag-and-drop selected software updates, or an update list, to a deployment template. The deployment will be preconfigured with settings from the deployment template and will only ask for the target collection (if not already set in the template), deployment package (if the update is not already part of an existing package), deployment schedule, and Network Access Protection effective date (if NAP is enabled).
 - Drag-and-drop selected software updates, or an update list, to a deployment. The preconfigured settings for the deployment are maintained, and the wizard will only ask for information about the deployment package (if update is not in an existing package), download location (if update is not in an existing package), deployment schedule, and NAP effective date (if NAP is enabled).
 In this example, we used the update list for Critical Security Updates for Windows 2000 that we created earlier in the chapter. The first page of the Deploy Software Updates Wizard is shown in Figure 7.44.
- 4. The first page is very straightforward. Give a name for your deployment, add a description, and click Next.

FIGURE 7.44
The General page



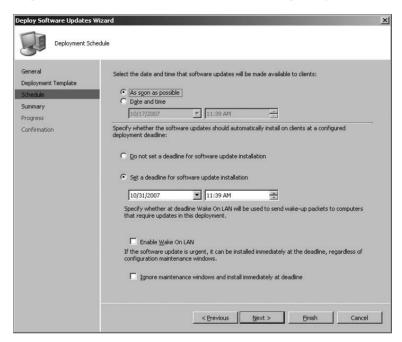
5. The Deployment Template page is next in line, as shown in Figure 7.45. From this page you can either select an existing deployment template, or create a new deployment definition. For this example, you will select the deployment template that you made earlier in the chapter, Windows 2000 Professional Systems, and click Next.

FIGURE 7.45Deployment Template page



- **6.** The Deployment Schedule page is next, and is shown in Figure 7.46. This page has two sections:
 - Select the date and time that software updates will be made available to clients: As Soon As Possible (the default) or Date And Time, which allows you to set a specific date and time that clients will be able to see the deployment. The latter is a good option if the updates have not made it to all of the distribution points yet.

FIGURE 7.46Deployment Schedule page



- Specify whether the software updates should automatically install on clients at a configured deployment deadline:
 - ◆ Do Not Set A Deadline For Software Update Installation.
 - Set A Deadline For Software Update Installation. Enabled by default, this
 allows you to set a date and time as a deadline for this deployment to be
 installed on clients.
 - Enable Wake On LAN. Disabled by default, this specifies whether at deadline Wake On LAN will be used to send wake-up packets to computers that require updates in the deployment.
 - ◆ Ignore Maintenance Windows And Install Immediately At A Deadline. If the software update is urgent, it can be installed immediately at the deadline, regardless of configuration maintenance windows. This option is disabled by default.

Once you have made your choices on this page, click Next.

7. On the Summary page, you can review the options you selected. If you are using update lists and deployment templates, it is a good idea to look the summary over to make sure

the deployment is going to do what you expect it to. After you have finished reviewing the Summary, click Next, and when the progress bar is done, click Close.

Monitoring Software Update Deployments

There are two main phases to the software deployment process that is performed by Configuration Manager client software:

Evaluation Configuration Manager clients determine if the software updates in a deployment are required.

Enforcement Clients report their compliance state for the deployment.

Microsoft provides excellent reports to monitor the phases of software update deployments in Configuration Manager 2007, and these reports are considered the best way to monitor the software update deployments. Those reports can be found in the Software Updates - C. Deployment States category in the Reports node in the Configuration Manager console.

To monitor the evaluation phase of software update deployments, you should use the following three main reports.

- **States 2 Evaluation states for a deployment** This report will give you a summary of the evaluation state of clients for a selected deployment, and will provide information as to whether clients were able to evaluate a deployment successfully.
- **States 4 Computers in a specific state for a deployment** <**secondary**> This report can be drilled down into to get more information about clients in a specified deployment state.
- **States 7 Error status messages for a computer** This report can be used to get all error message info for a deployment on a specific computer.

To monitor client enforcement for software update deployments, there are also three main reports that you should use.

- **States 1 Enforcement states for a deployment** This report gives a summary of the enforcement state of clients for a specific deployment. This report will show information on the state for installing the updates in the deployment, such as downloading the update, installing the update, successfully installed the update, and so on.
- States 4 Computers in a specific state for a deployment < secondary >
- States 7 Error status messages for a computer

To monitor the status of software update deployments to SMS 2003 clients, you can use the reports in the Software Updates - E. Distribution Status for SMS 2003 Clients category.



CONDITION CRITICAL

Now that you have deployed Configuration Manager and have Software Updates up and running, your manager wants you to make a concentrated effort to get clients up-to-date with Critical security

patches. He has made it clear that these are to be given priority over other updates until the numbers of required patches are down to a reasonable level, which is not the case now.

To accomplish your new software update initiative, you will first need to figure out what patches need to be installed on what computers.

One way to do this is to set up search folders for each operating system that you support, containing all the Critical security patches. With those search folders, you highlight all the security patches that are required by your clients and make an update list out of them.

Once you have done that, you can either download all the updates and get them onto your distribution points, or start a deployment directly from the update list and configure downloading those updates as part of that update.

The procedures that we have detailed earlier in the chapter for configuring the different elements of Software Updates were made with that method of organization in mind.

The Bottom Line

Plan to Use Software Updates You can use the same method of "deployment intelligence" that was used in Chapter 2, to gather information for planning to implement Software Updates. This will be very helpful in making sure that you get the most out of the Software Updates feature for your organization.

Master It What is the first step in gathering "deployment intelligence" for planning to implement Software Updates?

Configure Software Updates Before you can utilize Software Updates in your environment, the various components of this feature need to be set up and configured.

Master It What is the very first thing you have to install before you can use Software Updates?

Use the Software Updates Feature to Manage Software Updates The hardest thing to do in SMS 2003 relating to patch management was to programmatically prioritize software updates that are critical so they can be deployed with a higher priority than other updates.

Master It What does Configuration Manager provide that can help with prioritizing software updates?

Chapter 8

Operating System Deployment

Most IT administrators want to automate as many functions as possible in order to reproduce the same outcome consistently and quickly to as many devices as possible, and setting up a basic computer build is no exception. Microsoft Configuration Manager 2007 R2 has made massive strides in this area and can be classified as a feature-rich operating system deployment (OSD) package.

In this chapter, we will cover the basics of deploying an operating system using Configuration Manager 2007; there are many subtle differences between operating systems and various ways to deploy each of them using Configuration Manager 2007, a topic that could be a book of its own. In this chapter, you will learn how to do the following:

- Specify a Network Access account
- Set up a PXE service point
- Update the driver catalog package

Preparing Configuration Manager 2007 for OSD

Configuration Manager 2007 needs to be configured for deploying an operating system image. The first step in preparing for OSD is to install the User State Migration Tool (USMT) version 3.0 or higher. USMT is used to back up and restore user state information; it captures desktop settings, application settings, user accounts, and user files.

Setting Up the User State Migration Tool

First, download USMT from Microsoft's website; at the time of this writing, you can find the most recent version here:

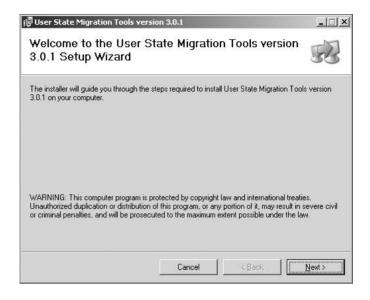
www.microsoft.com/downloads/details.aspx?FamilyId=799AB28C-691B-4B36-B7AD-6C604BE4C595&displaylang=en

- **1.** Run the setup program; the installation is pretty basic. After executing the download program, you are presented with the welcome screen, as shown in Figure 8.1.
- 2. Next you will be presented with the license agreement. You'll need to agree to the license agreement to proceed, so select I Agree, and then click Next.
- **3.** On the Confirm Installation wizard page, click Next to start the installation. When the installation process completes, click Close.

Now that USMT has been successfully installed, the USMT30 folder needs to be shared so that Configuration Manager can use the tool. You will need to share the folder C:\Program

Files\USMT30; in this case, share it as USMT. Also, make sure to grant administrators full control to the USMT share.

FIGURE 8.1
The User State Migration
Tools Wizard's welcome
screen



Configuring the Network Access Account

The next step is setting up an Active Directory user to be assigned as the Network Access account. A general rule for this account is to call it NetworkAccess so it is easily identifiable. So, have a domain administrator create an account called NetworkAccess (or whatever fits your environment's naming conventions).

After this Network Access account has been created, you will need to configure Configuration Manager 2007 to use the Network Access account. Take the following steps:

- Open the Configuration Manager console, and expand Site Database ➤ Site Management ➤ Site ➤ Site Settings ➤ Client Agents.
- 2. Right-click Computer Client Agent, and select Properties.
- **3.** Set the Network Access account to the account created earlier, and click OK, as shown in Figure 8.2.

Creating the Configuration Manager Client Install Package

The next step is to configure a package in order for the Configuration Manager 2007 client to be installed once the new operating system has been deployed to a new machine. This will ensure that the new machine gets the Configuration Manager client as soon as the machine comes online. There is nothing out of the ordinary about creating the package for the client:

- 1. Expand Site Database ➤ Computer Management ➤ Software Distribution ➤ Packages.
- 2. Right-click Packages, select New, and then click Package From Definition. This opens the Create Package From Definition Wizard's Welcome page, as shown in Figure 8.3.

FIGURE 8.2 Computer Client Agent Properties dialog box

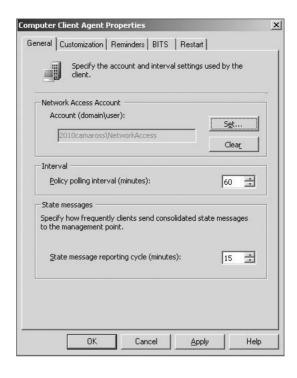
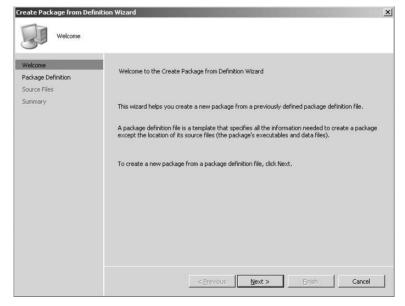
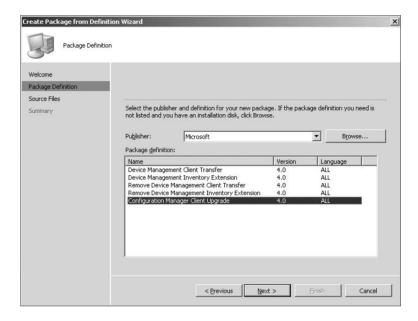


FIGURE 8.3Create Package From Definition Wizard's Welcome page



- 3. Clicking Next on the Welcome page brings you to the Package Definition page, shown in Figure 8.4. This allows you to select the Configuration Manager Client Upgrade package definition. After selecting the Configuration Manager Client Upgrade package, click Next.
- On the Source Files page, select Always Obtain Files From A Source Directory, and click Next.

FIGURE 8.4 Create Package From Definition Wizard's Package Definition page



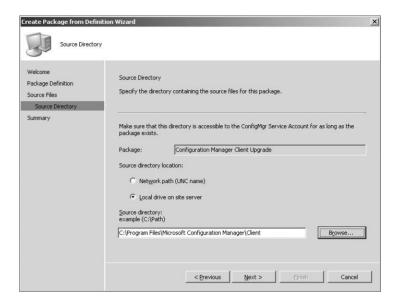
- 5. This opens the Source Directory page, shown in Figure 8.5, allowing you to designate the source file directory. In this dialog box, select Local Drive On Site Server, and fill or browse for the source directory. Click Next.
- **6.** On the Summary page, click Finish, and Configuration Manager 2007 will create the client upgrade package.

This package contains only one program, which is a silent upgrade install of the Configuration Manager 2007 client. You will want to specify a distribution point so you can deploy this package within your organization. Expand the package name, right-click, choose New Distribution Points, and then select the distribution points you want to use for this package.

Creating a USMT Package

Additionally, you will need to create a package that OSD will use to gather the entire user state and migrate it to the new environment. This is known as *user state migration*. The following procedures will demonstrate not only how to set up the USMT package but also how to set up the state migration point within Configuration Manager 2007. OSD will use the USMT to capture not only the user's settings but also the user's state at the time in which the package runs. This capture is known as the *scan state*. Configuration Manager then migrates this scan state and restores those settings, known as the *load state*, to the new system.





The steps for creating a USMT package are similar to those for creating packages that we have discussed earlier in this book:

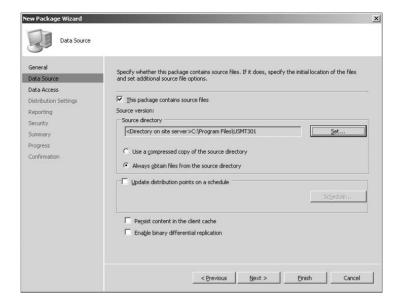
- **1.** Expand Site Database, and choose Computer Management ➤ Software Distribution.
- **2.** On the Software Distribution tab, select Packages. Right-click Packages, select New, and then click Package.
- **3.** The General page, shown in Figure 8.6, appears; fill in the name and other information as you see fit, and click Next.

FIGURE 8.6The New Package
Wizard's General page

New Package Wizard			×
General			
General Data Source Data Access Distribution Settings Reporting Security Summary Progress Confirmation	Name: Yersion: Manufacturer: Language: Comment: L It is reco	USMT USMT English USMT USMT	
		<pre></pre> <pre>< Previous</pre>	

4. On the Data Source page, shown in Figure 8.7, select the This Package Contains Source Files box, and select Set.

FIGURE 8.7
The New Package
Wizard's Data
Source page



- 5. The Set Source Directory page appears, allowing you to browse for the selected files. Browse to the folder where you installed USMT (the default location is C:\Program Files\USMT301), and then click OK.
- **6.** Click OK again to return to the Data Source page.
- **7.** After clicking Next on the Data Source page, you will be presented with the Data Access page. Accept the defaults, and click Next to continue.
- **8.** On the Distribution Settings page, click Next to accept the defaults, and click Next again on the Reporting page.
- **9.** Now you will be presented with the Security page. Select the security settings, and then click Next.
- **10.** You're almost finished. Click Next on the Summary page and then Close when you are prompted Wizard Completed page.

Now, remember you will need to assign a distribution point for this package. There is nothing different about assigning a distribution point for this package. Just expand the package, click Distribution Point, and select New Distribution Point from the Action pane.

USER STATE MIGRATION TOOL DOCUMENTATION

You can find the User State Migration Tool documentation here:

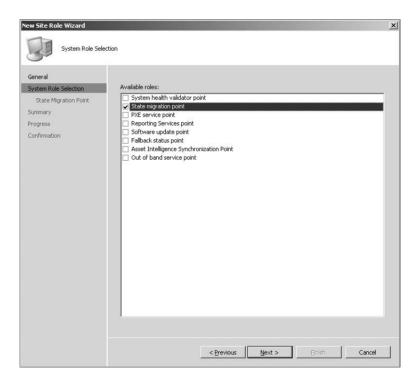
http://technet.microsoft.com/en-us/library/cc722032.aspx

Configuring the State Migration Point Role

The next step in preparing Configuration Manager 2007 for OSD is to set up a state migration point. The state migration point is used to store the migrated settings and data during the operating system image deployment. This state migration point is a site system role within Configuration Manager 2007 and will need to be assigned to a server. Follow these few steps to set up the state migration role:

- From within the Configuration Manager console, browse to Site Database ➤ Site Management ➤ Site Code ➤ Site Settings, and select Site Systems.
- 2. This presents a list of all the site systems configured within your environment. Expand Site Systems, and select the server to which you want to add the state migration point role. Right-click the server, and select New Roles.
- On the New Site Role Wizard's General page, click Next. You will be presented with the System Role Selection page, shown in Figure 8.8. Select State Migration Point, and click Next.

FIGURE 8.8 New Site Role Wizard's System Role Selection page



- **4.** On the State Migration Point page, shown in Figure 8.9, click the starburst icon to create a new storage folder.
- **5.** Creating a new storage folder on the Storage Folder page, shown in Figure 8.10, allows you to enter the path to use when storing state migration data.
- **6.** Clicking OK returns you to the State Migration Point page.

FIGURE 8.9 New Site Role Wizard's State Migration Point page

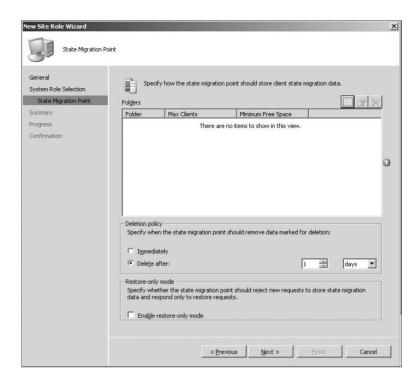
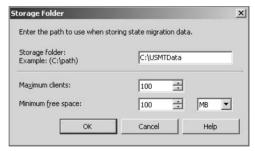


FIGURE 8.10 Designating a storage folder



- **7.** You can change the deletion policy if you think one day is too long or not long enough until the user data is removed from the state migration point. Click Next, and you will be taken to the Summary page.
- **8.** Click Next to allow Configuration Manager to create the new site role.
- **9.** This presents you with the Wizard Completed page; click Close.

Distributing the Boot Image Package

The final part of preparing Configuration Manager 2007 for operating system deployment is to distribute the boot image package to a distribution point. This boot image is used to start the computer in Windows Preinstallation Environment (WinPE) for capturing, prior to deploying the

operating system image. This procedure, because of the size of the images, will take some time to complete:

- 1. From within the Configuration Manager console, expand Site Database ➤ Computer Management ➤ Operating System Deployment, and select Boot Images.

 You will notice two boot images for various platforms, one for x64 bit (Boot Image [x64]) and the other for x86 devices. For the purpose of this book, we will concentrate on the x86 boot images, but there is basically no difference in configuring one or the other. The images are configured during the installation of Configuration Manager 2007. However, there are no distribution points assigned for either of the boot images.
- 2. To configure a distribution point, expand Boot Images ➤ Boot Image (x86), and click Distribution Points.
- **3.** Right-click Distribution Points, and select New Distribution Point. This opens the New Distribution Points Wizard's Welcome page; click Next to continue.
- 4. Select the distribution point you want to use on the Copy Package page, and click Next.
- **5.** Then on the Wizard Completed page, click Close. It will take some time to copy the boot image package up to the distribution point.

Let's review the steps briefly for configuring Configuration Manager 2007 for OSD. First, you installed the USMT, next you configured the network access account, and then you created the client install package. After creating the client install package, you set up a package for USMT and then set up the state migration point for Configuration Manager 2007. The final step was to deploy the boot images to the distribution points.

Developing a Task Sequence for Creating a Capture Image

Now we will show how to create a task sequence that will be used to capture an image of a work-station. A *task sequence* is a way for Configuration Manager 2007 to perform one or more steps or tasks on a client computer without requiring user intervention. A task sequence can consist of a single step or multiple tasks grouped together to perform functions. They can depend on other tasks to complete successfully or be independent of each other.

Take the following steps to create a task sequence for creating a capture image:

- In the Configuration Manager console, expand Site Database ➤ Computer Management ➤ Operating System Deployment.
- **2.** From within the Operating System Deployment node, right-click Task Sequences, and select Create Task Sequence Media. This opens the Select Media Type page, shown in Figure 8.11.
- **3.** On the Select Media Type page, select Capture Media, and then click Next. By selecting Capture Media, you will be creating the capture media that will be used to capture the operating system image.
- **4.** On the wizard's Media Type page, shown in Figure 8.12, you can select the type of media to create.
- 5. For this example, select CD/DVD Set, specifying the media file location, and click Next.

FIGURE 8.11
Task Sequence Media
Wizard's Select Media
Type page

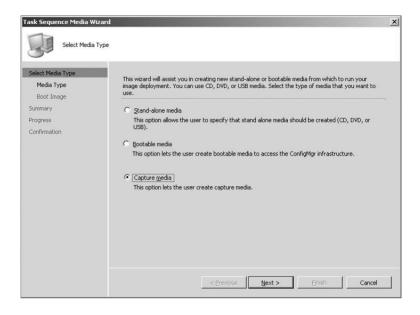
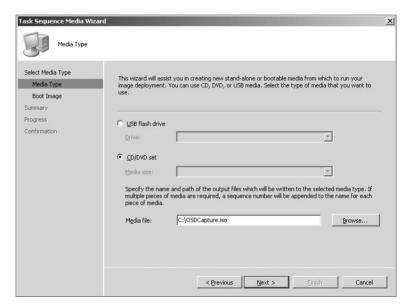
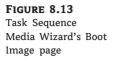
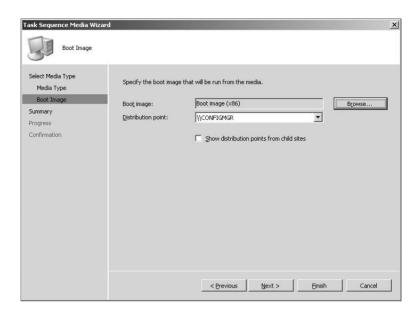


Figure 8.12
Task Sequence Media
Wizard's Media
Type page



- **6.** On the Boot Image page, shown in Figure 8.13, specify the boot image and distribution point you want to use. Click Browse, and select the boot image. Click Next to continue.
- Click Next on the Summary page, and Configuration Manager 2007 will begin creating the capture media ISO file.





8. Finally, you will be presented with the Wizard Completed page, where you can click Close. You can now burn that ISO file to a CD and use that CD to boot up the computers in which you will be building your operating system image.

Creating an Image of a Reference Computer

When creating an image of a reference computer, you need to be aware of a few issues. First, ensure that the computer is a member of a workgroup instead of a member of the domain. This is a required step; if the reference computer is a member of the domain, you will be required to remove it from the domain to create the image of the operating system of the computer. Second, we recommend removing the Configuration Manager client from the machine. This is not a requirement, just a recommendation. Another item that is recommended is to blank the local administrator password.

- To begin creating an image of the reference computer, insert the CD that was created from the OSDCapture. ISO file you created earlier. Run TSMBAutorun. exe located in the SMS\Bin\i386 folder on the CD. This opens the Image Capture Wizard, shown in Figure 8.14.
- **2.** Clicking Next opens the Image Destination page, shown in Figure 8.15, allowing you to specify where to copy the image when the capture is completed. Fill in the correct information, and click Next. As you can see, we copied the WIM file to our site server.
- **3.** You will now be able to add some information about the image on the Image Information page, shown in Figure 8.16. This page allows you to fill in the Created By, Version, and Description fields for the WIM file. It is recommended to fill this information in as much detail as you can; then click Next.

FIGURE 8.14 Image Capture Wizard

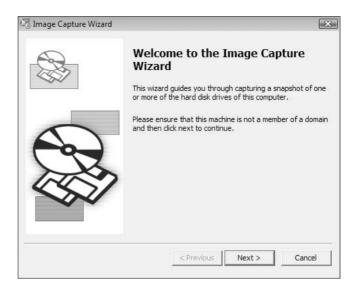


FIGURE 8.15 Image Capture Wizard's Image Destination page



4. On the Summary page, click Finish to begin the capture phase. An Installation Progress window appears, as shown in Figure 8.17, telling you that the capture wizard is working and running in the background. When the capture is complete, a System Restart message will appear, and the system will reboot. When the system reboots, it will boot into WinPE, as shown in Figure 8.18, and begin the capture phase of the system.

FIGURE 8.16 Image Capture Wizard's Image Information page

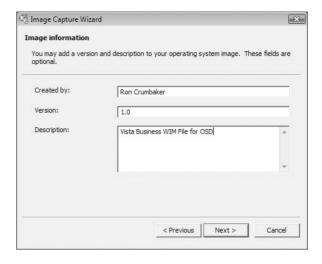
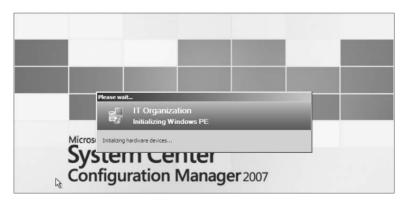


FIGURE 8.17
Configuration
Manager 2007 installation progress



FIGURE 8.18
Booting to WinPE



This process can be a lengthy one, so be patient while the operating system is being captured.

5. Once the image capture is complete, you will be prompted with the Image Capture Wizard success message, shown in Figure 8.19. Clicking OK will allow the machine to reboot and return to the operating system.

FIGURE 8.19 Image capture completion message

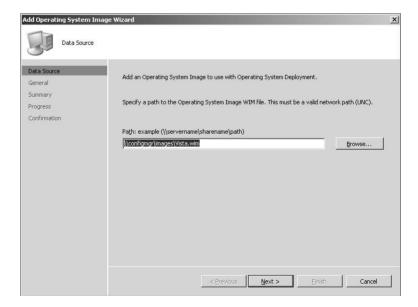


Packaging and Advertising the Image

Since you've successfully captured the image, next you need to configure the image as a new package and then as an advertisement and ultimately deploy it to another system:

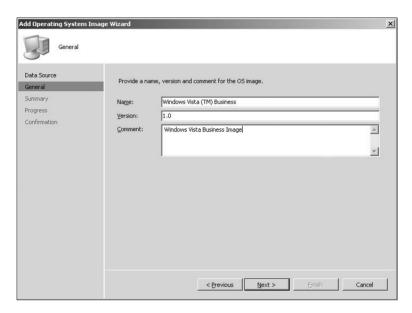
- Open the Configuration Manager console, and expand Site Database ➤ Computer Management ➤ Operating System Deployment.
- 2. The WIM file that you just created needs to be created as an available operating system for Configuration Manager 2007. To add this WIM file, click Operating System Images under the Operating System Deployment node, and click Add Operating System Image from the Action pane.
- **3.** This opens the Add Operating System Image Wizard's Data Source page, shown in Figure 8.20. Ensure that the Pathfield points to the location where the WIM file was created, and click Next.

FIGURE 8.20 Add Operating System Image Wizard's Data Source page



4. The General page, displayed in Figure 8.21, allows you to customize the Name, Version, and Comments fields for the image file. Fill in the appropriate information, and click Next.

FIGURE 8.21
Add Operating
System Image
Wizard's General page



5. The Summary page will be displayed, so click Next, and then finally the Wizard Completed screen will appear. On this page, click Close.

Distributing and Deploying the Image

Next, you need to configure a distribution point in order to distribute this image. This step is a little different from the steps for assigning distribution points for packages we discussed elsewhere in this book:

- Expand Site Database ➤ Computer Management ➤ Operating System Deployment ➤ Operating Systems Images, and expand the image, which in this case is Windows Vista (TM) Business.
- 2. You will see the same node structure under this package as you would for a normal package. Right-click the Distributions Point node, and select New Distribution Point. The same New Distribution Point Wizard will display, allowing you to select the distribution point you want to use to distribute the image file.
- **3.** To verify that the package has been successfully installed on the distribution point, while in the Operating System Images node, expand the Windows Vista (TM) Business folder, expand the Package Status node, and click the Package Status folder.
 - Within this folder, you will see the status of the package. When the package has been successfully installed on the distribution point, the Installed column will change from 0 to 1, as shown in Figure 8.22.

FIGURE 8.22 Verifying successful package installation

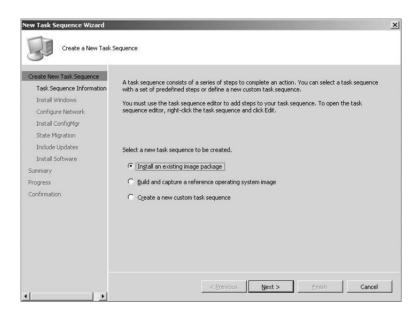
Site	Source Version	Targeted	Installed	Retrying	Failed	Summ
255 - 2010 Camaro SS	1	1	1	0	0	12/22,

Developing a Task Sequence for Deployment

Now you will need to create a task sequence for deploying the Windows Vista operating system image. Creating a task sequence will give Configuration Manager 2007 a series of steps to perform on the new installation of the workstation:

- First expand Site Database from the Configuration Manager console; then expand Computer Management ➤ Operating System Deployment, and click the Task Sequence node.
- 2. Right-click Task Sequence, and select New ➤ Task Sequence. This opens the New Task Sequence Wizard's Create A New Task Sequence page, shown in Figure 8.23.

FIGURE 8.23 New Task Sequence Wizard's Create A New Task Sequence page



- Because you have already built an image of a Vista client, you will select Install An Existing Image Package and then click Next.
- **4.** This opens the New Task Sequence Wizard's Task Sequence Information page, shown in Figure 8.24, allowing you to specify the task sequence name and a comment and to specify the boot image to use during the installation.
- 5. The Install The Windows Operating System page, shown in Figure 8.25, allows you to specify the Configuration Manager 2007 image package containing the operating system you want to install. Click the Browse button to find the image of the operating system you want to install, and click OK.

FIGURE 8.24
New Task Sequence
Wizard's Task Sequence
Information page

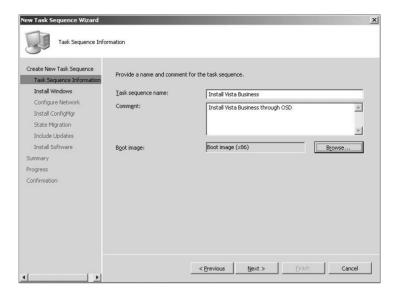
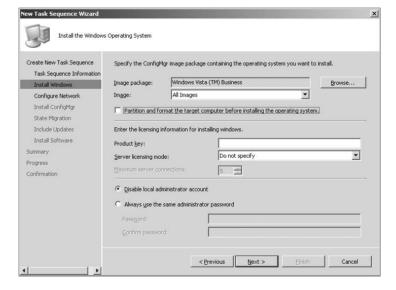
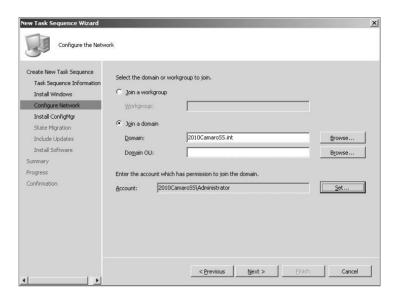


FIGURE 8.25 New Task Sequence Wizard's Install Windows page



- **6.** If you want to partition and format the target computer before installing the operating system, leave the Partition box selected, and format the target computer before installing the operating system. Enter the licensing information for the version of Windows you are installing in the Product Key field, and click Next.
- **7.** On the Configure The Network page, shown in Figure 8.26, you can select the domain or workgroup to join. If you select to join a domain, you can specify which OU to put the computer in once it joins the domain. If you select to join a domain, you will need to specify the account that has permission to join computers to a domain. Click Next to continue.

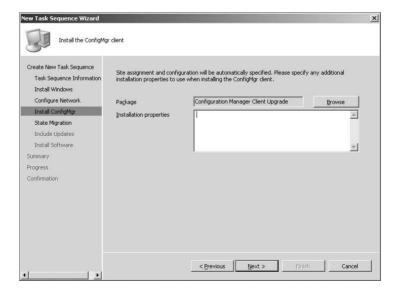
FIGURE 8.26 New Task Sequence Wizard's Configure The Network page



Now all the work you did earlier will finally be put to use.

8. On the Install The ConfigMgr Client page, shown in Figure 8.27, you can specify any additional packages you want to install once the operating system has been installed on the workstation. This will allow you to use the Configuration Manager Client Upgrade you configured earlier in this chapter. Click the Browse button, select Configuration Manager Client Upgrade, and click OK.

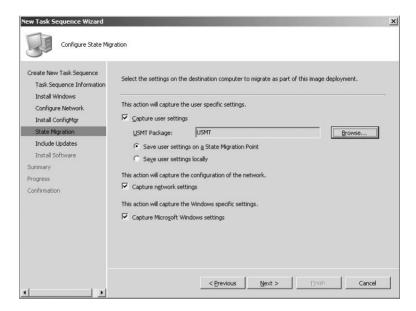
FIGURE 8.27 New Task Sequence Wizard's Install The ConfigMgr Client page



This brings you back to the Install The ConfigMgr Client page, where you can specify additional installation properties. Then click Next to continue.

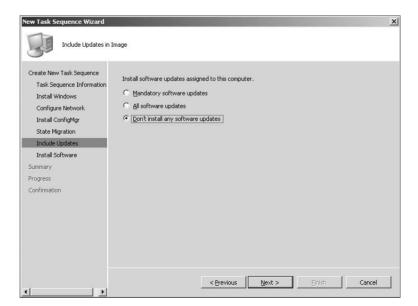
10. The New Task Sequence Wizard page that appears is Configure State Migration, shown in Figure 8.28, which allows you to configure the user state migration capture. Click Browse, select the USMT package created earlier in this chapter, and then click Next.

FIGURE 8.28 New Task Sequence Wizard's Configure State Migration page



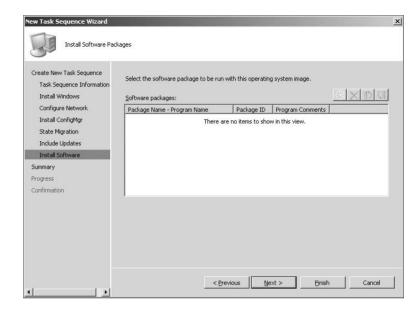
11. After you've configured the state migration, the Include Updates In Image page, shown in Figure 8.29, allows you to specify whether the client will get mandatory, all, or no software updates after the image has been installed.

FIGURE 8.29 New Task Sequence Wizard's Include Updates In Image page



12. Now you have the option to install additional software packages by adding the configured packages to the task sequence. This is extremely useful if you have a large number of applications you want installed on each system after the operating system has been installed. Figure 8.30 shows the Install Software Packages page, where you can specify the additional packages. Select Next once you have them configured.

FIGURE 8.30 New Task Sequence Wizard's Install Software Packages page



13. Click Next on the Summary page, and Configuration Manager 2007 will complete the New Task Sequence Wizard and allow you to click Close.

Advertising the Task Sequence

Now you have successfully created a new task sequence to install a new operating system on a machine along with joining the system to the domain and installing the Configuration Manager 2007 client on the machine once it comes online. However, the task sequence will not do any good unless you advertise it to a collection. Take the following steps:

- To advertise the task sequence, select the Install Vista Business task sequence from the Task Sequence node in the Configuration Manager console.
- **2.** Then, in the Actions pane, under Install Vista Business, click Advertise. This opens the General page, shown in Figure 8.31.
- 3. Browse to find the collection where you want to install this operating system package, and then click Next to continue. You will need to specify when the program will be advertised to the members of the collection; when you have configured this, click Next.
- 4. The next wizard page is Distribution Points, shown in Figure 8.32. This will allow you to specify how clients interact with distribution points to retrieve content from packages referred by the task sequence. Click Next to continue.

FIGURE 8.31
New Advertisement
Wizard's General page

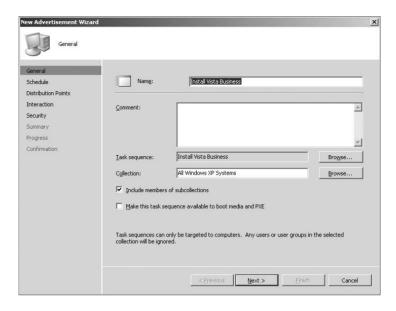
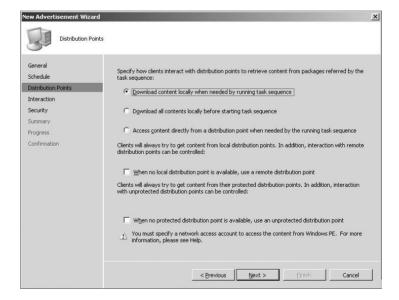
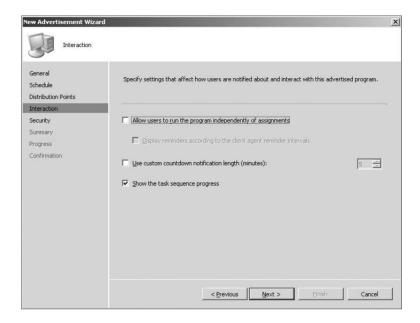


FIGURE 8.32 New Advertisement Wizard's Distribution Points page



- **5.** On the Interaction page, shown in Figure 8.33, specify how users are notified about the advertisement and how they interact with the advertisement. We prefer to show the task sequence progress to let the end user know the computer is being reloaded.
- **6.** On the Security page, specify the correct rights for your environment, and then click Next. This brings you to the Summary page, and then finally after clicking Next, you will have successfully advertised the package. Click Close to finish the process.

FIGURE 8.33New Advertisement
Wizard's Interaction
page

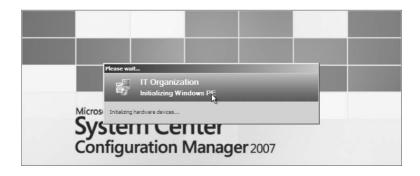


Now you have advertised the operating system deployment, and any system in the collection you specified will get the new advertisement during the next policy refresh. Once the policy refresh takes place, the workstation will be presented with the Assigned Program About To Run notification. Once the installation begins, you will see the Installation Progress message box, shown in Figure 8.34. The system will automatically reboot and then begin the boot to WinPE, shown in Figure 8.35.

FIGURE 8.34
New Advertisement
Wizard's Installation
Progress message box



FIGURE 8.35
Booting to WinPE

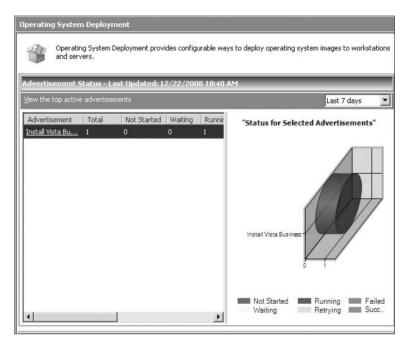


The installation will take some time to complete. During this install, Configuration Manager is gathering the user state and saving the date in the USMT folder on the site server, which you configured earlier in this chapter. You can monitor the C:\USMTData folder on the site server to see the user state migration data being copied to the server.

Configuration Manager will push the new operating system down to the new machine and then join it to the domain, install the Configuration Manger client, and finally reset all the user data on the client.

You can monitor the progress of the operating system deployment by choosing Run Home Page Summarization from the task pane on the Operating System Deployment node of the Configuration Manager console. This will show you the Advertisement Status window, shown in Figure 8.36.

FIGURE 8.36Monitoring the OSD advertisement status



Deploying the Operating System on "Bare Metal"

You have now successfully configured Configuration Manager 2007 for operating system deployment, prepared and captured a Vista client as a reference system, created a task sequence for deploying the newly created image, and finally, upgraded a Windows XP client to Vista. At the same time, you joined the client to the domain, saving the user's settings, and installing the Configuration Manager client on the new operating system for that machine.

However, you might be thinking, what if I have all these new machines without *anything* on the systems, just a blank bare-metal machine? How can I get Configuration Manager 2007 to install an image on those machines?

Creating PXE Service Points

To allow for Configuration Manager 2007 to use OSD for deploying to bare-metal devices, you need to use PXE service points, for which you will need to set up the Network Access account,

which you did earlier in this chapter. You will also need to ensure that the Configuration Manager Client Upgrade package has been configured and ready for deployment, as you also did earlier in this chapter. Finally, you need to ensure that the boot image is set up as a package.

Installing an operating system using a PXE service point requires that you create a PXE service point in your Configuration Manager site. This PXE service point must be installed on a Windows Deployment Server (WDS).

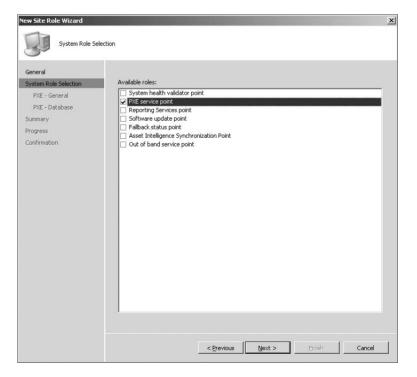
INSTALLING WINDOWS DEPLOYMENT SERVER

You can install Windows Deployment Server through Add Or Remove Programs on Windows 2003 SP2 or higher machines. For older operating systems, please check out http://technet.microsoft.com/en-us/library/cc772106.aspx for more information on setting up Windows Deployment Server.

The next stage in preparing Configuration Manager 2007 for OSD is to set up a PXE site service point. Follow these steps to set up the PXE site service role:

- From within the Configuration Manager console, browse to Site Database, then expand Site Management ➤ Site Code ➤ Site Settings, and select Site Systems.
- 2. This presents a list of all the site systems configured within your environment. Expand the Site Systems node, and select the server to which you want to add the role of PXE site service point. Right-click the server, and select New Roles.

FIGURE 8.37 New Site Role Wizard's System Role Selection page



- 3. On the New Site Role Wizard General page, click Next.
- **4.** You will be presented with the System Role Selection page. Select PXE Service Point, and then click Next, as shown in Figure 8.37.
- **5.** You will see the PXE Service Point Configuration dialog box, shown in Figure 8.38. This dialog box informs you that Configuration Manager 2007 must have some UDP ports opened on the server. Click Yes to continue enabling a PXE service point.

FIGURE 8.38
New Site Role Wizard's
PXE Service Point
Configuration dialog box

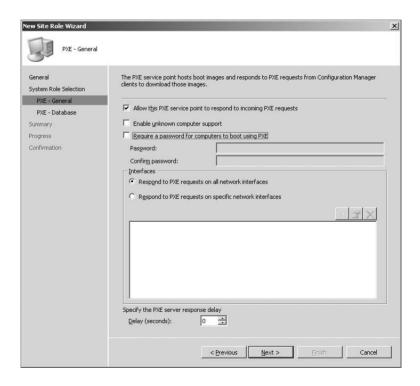


6. The New Site Role Wizard continues and presents the PXE – General page, shown in Figure 8.39. This will allow you to configure how Configuration Manager allows incoming PXE requests. Click Next when you're done.

FIGURE 8.39

New Site Role Wizard's

PXE – General page

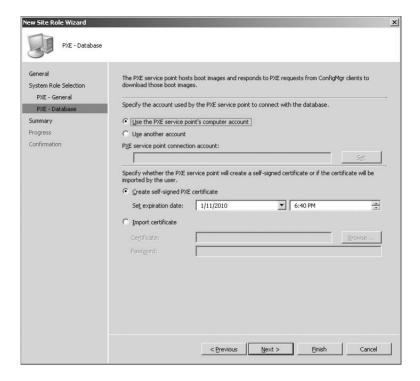


7. Next the PXE – Database page appears (Figure 8.40), allowing you to configure the account to use to connect with the database.

We strongly recommend allowing Configuration Manager to use the computer account to access the Configuration Manager site database when validating clients. This will prevent

a lot of headaches when you need to change passwords because of an audit or some policy within your organization.

FIGURE 8.40 New Site Role Wizard's PXE – Database page



- **8.** After you have configured the settings on this page, click Next.
- On the Summary page, click Next to apply the settings, and configure the PXE service point.

It will take some time for the PXE service point to successfully install on the system. You can monitor the progress of the installation by checking the PXESetup.log file. You will need to distribute the boot image packages to the PXE service point as you did earlier in this chapter when you were configuring the state migration point.

If you install the PXE service point on a member server or a server that is not already an SMS site system, the PXE service point will install a limited distribution point role for hosting a boot image. This limited distribution point will be used only for the PXE service point and will create a folder called SMSPXEImages\$ on the server.

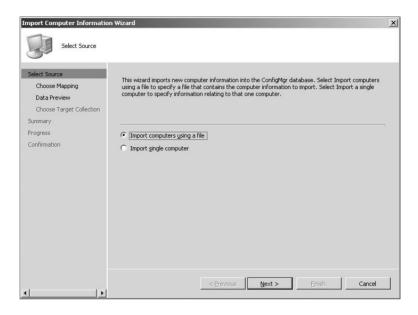
Setting Up a Computer Association

Now you are ready to set up a computer association so that Configuration Manager can identify the bare-metal machines that will receive a fresh install. To specify the computer association, you will need to open the Configuration Manager console and proceed as follows:

1. Expand Site Database ➤ Computer Management ➤ Operating System Deployment, and finally click Computer Association.

2. Right-click Computer Associations, and select Import Computer Information to display the wizard shown in Figure 8.41.

FIGURE 8.41
The Import Computer Information Wizard



3. This will allow you to enter a single computer or import many systems from a comma-separated values (CSV) file. Selecting the option Import Single Computer will present you with the Single Computer page, as shown in Figure 8.42.

FIGURE 8.42 Import Computer Information Wizard's Single Computer page

elect Source	Specify information relating to the computer you are importing in the fields below.	
Single Computer Data Preview		
Choose Target Collection	Computer name:	3
immary	MAC address (12 hex characters):	
rogress		
onfirmation	SMBIOS GUID (32 hex characters):	- 1
	Optionally create a computer association by entering the name of a reference computer from the user state and settings will be migrated to the new computer	m which
	the user state and settings will be migrated to the new computer	m which earch
	the user state and settings will be migrated to the new computer	
	the user state and settings will be migrated to the new computer	

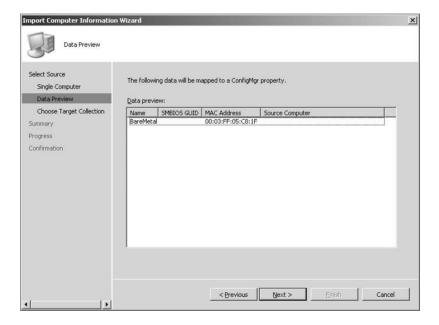
You are required to enter the computer name along with either the MAC address or the SMBIOS GUID. The computer name is just how the machine will appear in the collections, not what the actual computer will be named.

DHCP AND PXE

You'll need to set up some DHCP options for PXE to boot properly. You will need to specify options 60, 66, and 67. Option 66 enables PXE support, option 66 is the FQDN of the Configuration Manager server, and option 67 should be the path pxeboot.com.

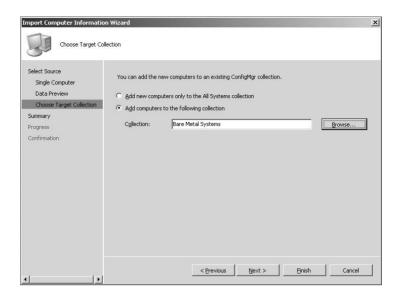
4. Fill in the appropriate information, and then click Next. This presents you with the Data Preview page, shown in Figure 8.43.

FIGURE 8.43 Import Computer Information Wizard's Data Preview page



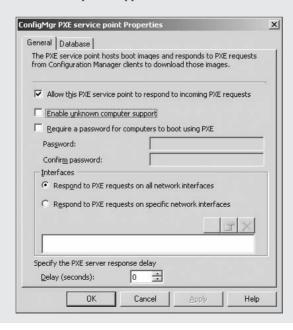
- **5.** After clicking Next on the Data Preview page, you'll see the Choose Target Collection page, shown in Figure 8.44. Here you can specify which collection you want to add this new machine. It is extremely valuable to put all the bare-metal installs into the same collection so you can find them more easily.
- **6.** After specifying the collection, you are presented with the Summary page. Click Next and then Close on the Finish page.

FIGURE 8.44
Choosing a target collection



USING THE UNKNOWN COMPUTER COLLECTION

You can enable support for unknown computers. Unknown computers is a feature within the R2 version of Configuration Manager 2007 that will allow unmanaged systems the ability to be managed with Configuration Manager 2007 during an OS Deployment. To do so, open the Configuration Manager console, and expand Site Management \triangleright site code \triangleright Site Settings \triangleright Site Systems. Click the server that has the ConfigMgr PXE service point, and expand it. Right-click ConfigMgr PXE Service Point, and choose Properties. In the ConfigMgr PXE Service Point Properties dialog box, shown here, select the box Enable Unknown Computer Support.

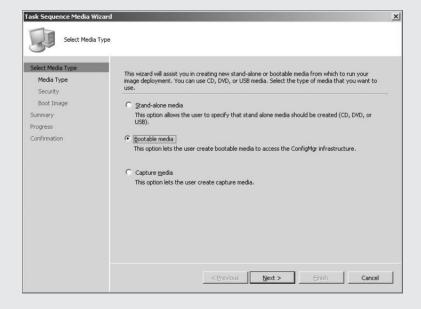


When you enable this option, you will be prompted with the caution message shown next. Assuming you are ready to proceed, click OK.

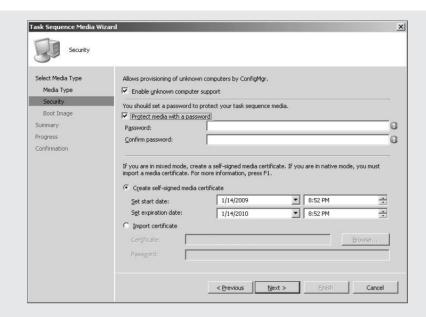


This creates a new collection called All Unknown Computers. To use this unknown computer support for media-booting systems, you will need to select the Enable Unknown Computer Support box when you are creating your task sequence for bootable media.

To create a task sequence for bootable media, open the Configuration Manager console, and expand Site Database > Computer Management > Operating System Deployment > Task Sequences. Right-click Task Sequence, and select Create Task Sequence Media. This opens the Task Sequence Media Wizard's Select Media Type page.



Select Bootable Media, and click Next. In the Media Type dialog box, select the type of media you will be using, either a USB flash drive or a CD/DVD set, and then click Next. In the Security dialog box, you have the Enable Unknown Computer Support option. This will allow you to target the unknown computer collection with the operating system deployment.



Now you can create an advertisement to this collection for the OSD task sequence, and Configuration Manager will process the task sequence for the "unknown computers."

Creating a Task Sequence for the Bare-Metal OSD

Now that you have the new bare-metal machine identified, the next task is to create a task sequence for deploying an operating system onto this device using the PXE service point and then advertise that task sequence to the collection containing the new machine.

Creating a task sequence to deploy an image using Configuration Manager is one of the best additions to Configuration Manager from the old versions of Systems Management Server (SMS). Creating a task sequence for deploying an image to a new machine is very straightforward:

- Expand the console to the Site Database ➤ Computer Management ➤ Operation System
 Deployment ➤ Task Sequences node.
- **2.** From there, right-click Task Sequence, and select New Task Sequence. This opens the Create A New Task Sequence page of the New Task Sequence Wizard, shown in Figure 8.45. Select the Install An Existing Image Package option, and click Next.
- **3.** On the Task Sequence Information page (Figure 8.46), fill in the name, optionally add a comment, and select the boot image you want to use for the operating system deployment.
- **4.** On the Install The Windows Operation System page (Figure 8.47), select the image package by browsing to select the correct image. Because this example is deploying Vista to a bare-metal machine, you will enable the option to partition and format the target computer.

Figure 8.45 New Task Sequence Wizard's Create A New Task Sequence page

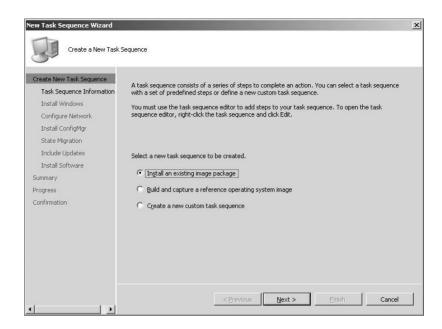
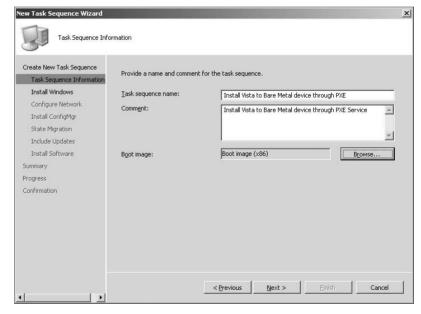


Figure 8.46 New Task Sequence Wizard's Task Sequence Information page



- **5.** The next options you can configure are the network settings. On the Configure The Network page, shown in Figure 8.48, specify whether you want to join the new machine to the domain or whether you want to join a workgroup.
- **6.** A Configuration Manager task sequence will allow you to install the Configuration Manager client during an operating system deployment. So, on the Install The ConfigMgr Client

page, shown in Figure 8.49, select the client installation package you created earlier in this chapter, and click Next.

FIGURE 8.47 New Task Sequence Wizard's Install The Windows Operating System page

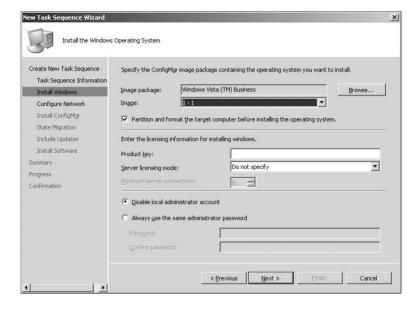
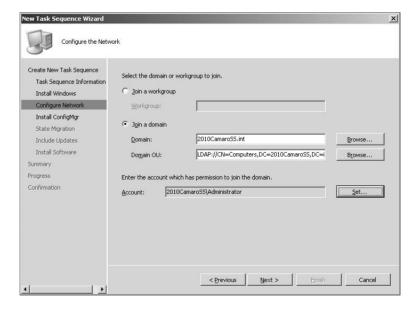


FIGURE 8.48
New Task Sequence
Wizard's Configure
The Network page



7. Since you are deploying Windows Vista to a bare-metal machine, on the Configure State Migration page, shown in Figure 8.50, you will unselect all the options because you do not need to worry about capturing any data from these machines.

FIGURE 8.49
New Task Sequence
Wizard's Install The
ConfigMgr Client page

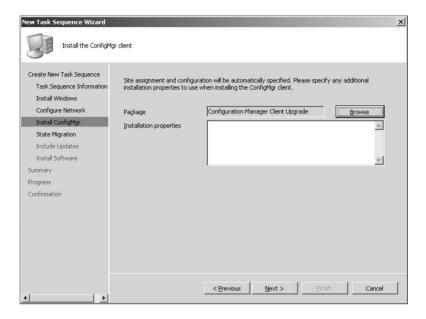
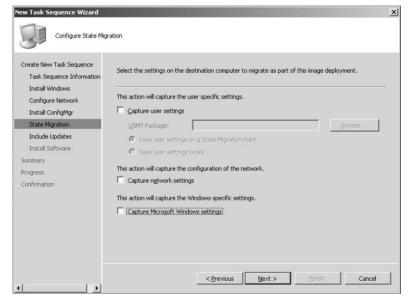
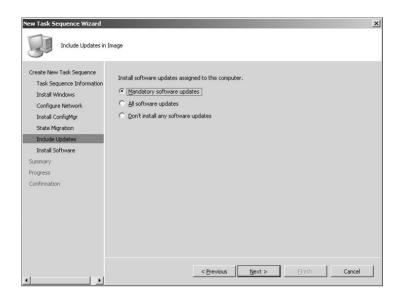


FIGURE 8.50 New Task Sequence Wizard's Configure State Migration



- **8.** On the Include Updates In Images page (Figure 8.51), you can now allow Configuration Manager to include software updates during the install. Make the selections as you desire, and click Next.
- **9.** If you have any additional packages you want to deploy, such as Microsoft Office or anything else, on the Install Software Packages page you can add any packages to install on the machine after the operating system has been deployed. Click Next on the Summary page and finally Close to complete the wizard.

FIGURE 8.51 New Task Sequence Wizard's Include Updates In Image page



Advertising the Bare-Metal Task Sequence

Now you need to advertise this task sequence to your Bare Metal collection so Configuration Manager will deploy the new operating system to the clients:

- 1. Under the Task Sequence node, select the Install Vista To Bare Metal Device Through PXE task sequence you just created, and in the Actions pane, select Advertise.
- 2. This is basically the same procedure as advertising any package to a machine; however, on the General page, shown in Figure 8.52, select the Make This Task Sequence Available To Boot Media And PXE, and then click Next.

FIGURE 8.52General New Advertisement Wizard

New Advertisement Wizard			x
General			
General Schedule	Name:	Install Vista to Bare Metal device through PXE	
Distribution Points Interaction Security	⊆omment:		
Summary Progress			
Confirmation	<u>T</u> ask sequence;	Install Vista to Bare Metal device through PXE	Browse
	Collection:	Bare Metal Systems s of subcollections	Browse
	✓ Make this task s	equence available to boot media and PXE	
	Task sequences can collection will be igno	only be targeted to computers. Any users or user groups ored.	in the selected
		< Previous Next > Einish	Cancel

All the other settings are the same as discussed earlier in this chapter. Now Configuration Manager 2007 is ready to deploy an operating system through PXE to bare-metal machines!

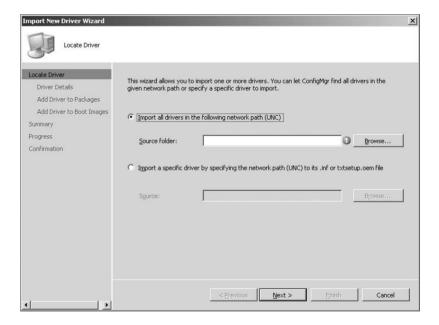
Installing Device Drivers into OSD

Now you have configured a package to perform Windows Vista upgrades and then another package to install that same Windows Vista install package onto a bare-metal system. However, what happens if you get a new system with a completely new setup, including device drivers that are not installed within the current package so that when the machine comes online it will not be able to attach to the network?

Microsoft has provided the ability to import device drivers into Configuration Manager 2007 and add them to the boot images or driver packages so they can be installed as part of the operating system deployment task. To import Windows device drivers, take the following steps:

- Expand the Configuration Manager console to the Site Database ➤ Computer Management
 ➤ Operating System Deployment ➤ Divers node.
- **2.** Right-click the Drivers node, and select Import. This opens the Locate Driver page, shown in Figure 8.53.

FIGURE 8.53 Import New Driver Wizard's Locate Driver page



- **3.** You can specify to import all drivers or just a single device driver. Click Next after picking the correct driver(s), and then you will be presented with the Driver Details page, shown in Figure 8.54, allowing you to name the driver differently or to use the one provided by the manufacturer and select a category if you choose.
- **4.** Figure 8.55 displays the Applicability page, where you specify on what platforms this driver can be installed. Ensure the settings are correct, and click Next.

FIGURE 8.54 Import New Driver Wizard's Driver Details page

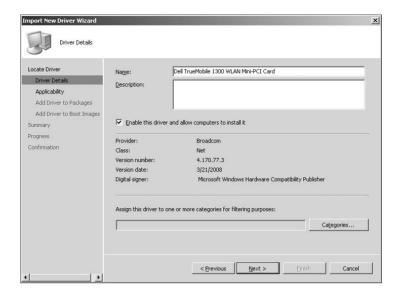
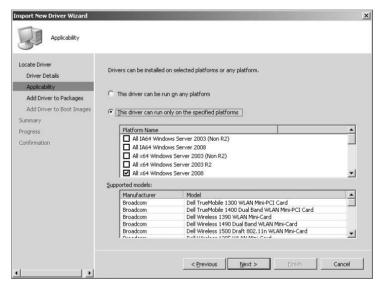


FIGURE 8.55 Import New Driver Wizard's Applicability page



- **5.** On the Add Driver To Packages page, shown in Figure 8.56, specify the package (s) you want to add this driver to, or specify a new package. If desired, select Update Distribution Points When Finished so the driver will be available as soon as possible to your site.
- **6.** Next you can select which boot images you want to add the driver to, as shown in Figure 8.57. Clicking Next presents you with the Summary page, where you click Next and then Close.
- **7.** Now Configuration Manager will go and inject that driver package to the packages and boot images you selected. This could take some time to process.

FIGURE 8.56 Import New Driver Wizard's Add Drivers To Packages page

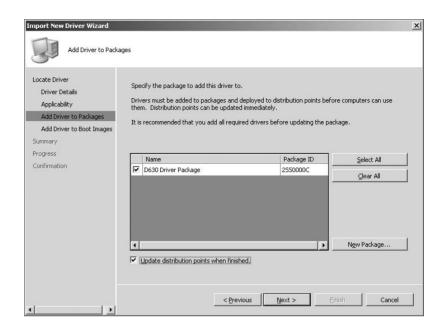
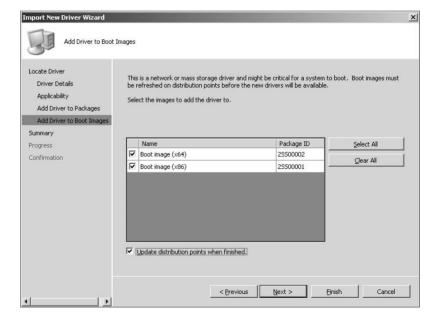


FIGURE 8.57
Adding drivers to boot images



Real World Scenario

ASSIGNING MANY COMPUTERS TO THE BARE-METAL DEPLOYMENT

George T. Management sends an email to the help desk stating that his department just ordered 10 new machines with no operating system and that he wants them all configured by the end of the day with the same image that was used on his machine. The list of 10 machines was included in the email.

You meet with your Configuration Manager team and decide that the best way to do this would be to use Configuration Manager to push the image out using the PXE service point that has already been used in the environment.

So, you open the Configuration Manager console, expand Site Databases > Computer Management > Operating System Deployment, and select Computer Associations. You right-click the Computer Associations node and select Import Computer Information. On the Import Computer Information page, you select Import Computers Using A File, and click Next. On the Choose Mappings page, you click Browse to browse the comma-separated file that Mr. Management sent you containing the list of computers you need to deploy the new operating system onto.

After you import the file and assign the data mappings, you click Next. Then you verify the data is correct on the Data Preview page and then add these systems into the Bare Metal collection created earlier with the Vista Business build already assigned. Finally, you click Finish to add the members to the collection. Configuration Manager will then deploy the new operating system when the machines are powered on and booted up in PXE boot.

The Bottom Line

Specify a Network Access account. The Network Access account is the account Configuration Manager will use to access the system while running WinPE.

Master It How do you specify the Network Access account?

Set up a PXE service point. A PXE service point is used by Configuration Manager to begin the operating system deployment process. The PXE service point responds to Configuration Manager clients making PXE boot requests.

Master It How do you set up a PXE service point?

Update the driver catalog package. The driver catalog will allow you to add drivers to the already created packages and images you have within your organization so you are not constantly re-creating your images when you get a new machine in your environment.

Master It How do you update the driver catalog package?

Chapter 9

Asset Intelligence

In May 2006, during the Microsoft Management Summit of that year, Microsoft announced the acquisition of AssetMetrix, a company that offered an online managed service for tracking computer resources.

About a year later, AssetMetrix technology had been integrated into SMS 2003 Service Pack 3. This technology, called Asset Management, extended the capabilities of SMS 2003 by bringing detailed asset inventory information such as expanded software usage metering, license management, and PC refresh and life-cycle management. With the Asset Intelligence Management database leveraged with software and hardware inventory, this new feature was able to provide more security assessment and verification as well as hardware configuration and hardware recalls information that wasn't available before.

The information from AssetMetrix in the form of Asset Management was merged with existing SMS 2003 tables, allowing for numerous detailed reports on software, hardware, and license management that were not previously possible. This capability made SMS 2003 even more valuable as a tool to manage computer resources in an enterprise environment.

This continued in Configuration Manager 2007, as the next version of Asset Management, now called Asset Intelligence, was revised and expanded for the latest release of the System Center line of products. Starting with Configuration Manager SP1, Microsoft added a wealth of functionality that allows users to customize Asset Intelligence to even further meet the needs of tracking assets in their organization; essentially, Asset Intelligence has become a fully realized feature of Configuration Manager.

In this chapter, you will learn how to do the following:

- Enable Asset Intelligence
- Enable Client Access License tracking
- Configure the Asset Intelligence Synchronization Point

What's New in Asset Intelligence in Configuration Manager

Asset Intelligence has been enhanced significantly in Configuration Manager 2007. New reports have been added to the Asset Intelligence Hardware, Software, and License Management categories. (We covered some of the other improvements to Asset Intelligence in Chapter 4.)

Besides tracking installed software, autostart software, and browser helper objects, new software reports provide information about recently used executables, and new hardware reports track processor age, USB devices, and readiness for an upgrade. You'll also find reports to identify computers that have software or hardware changes since the last inventory cycle. There are also

new Client Access License (CAL) reports added to the existing License Ledger reports, complete with the ability to compare license usage with Microsoft License Statements.

Configuration Manager SP1 added significant enhancements to Asset Intelligence, including the following:

- New catalog and license management capabilities from inside the Configuration Manager console.
- ♦ More reports.
- Asset Intelligence catalog synchronization to child sites.
- ◆ The ability to import both Microsoft and non-Microsoft software licensing data.
- The ability for Microsoft Software Assurance (SA) customers to dynamically update the Asset Intelligence catalog using the new Asset Intelligence synchronization point site system role

Requirements for Asset Intelligence

The Asset Intelligence feature in Configuration Manager 2007 has both external and internal dependencies that will need to be considered when using Asset Intelligence. Those requirements include the following:

- ♦ Client agent requirements
- ♦ Modification of the MOF that defines what is collected by hardware inventory
- Site maintenance task requirements
- Windows event log requirements

Client Agent Prerequisites

The Asset Intelligence reports are based on information gathered through hardware and software inventory. To get the necessary information from clients for all Asset Intelligence reports, you must enable these client agents:

- Hardware Inventory Client Agent
- Software Metering Client Agent

HARDWARE INVENTORY CLIENT AGENT REQUIREMENT

To be able to collect the majority of data for Asset Intelligence reports, the Hardware Inventory Client Agent must be enabled, and some of the hardware inventory classes contained in the sms_def.mof and configuration.mof files on the primary site servers must also be enabled. We will discuss this in more detail later in the chapter.

For more detail on hardware inventory file modification, see Chapter 10.

REPORTS THAT REQUIRE SOFTWARE METERING

Six reports require the Software Metering Client Agent to be enabled before they can provide any data:

- Software 07A: Recently Used Executables by Number of Computers
- Software 07B: Computers That Recently Used a Specified Executable

- ◆ Software 07C: Recently Used Executables on a Specific Computer
- Software 08A: Recently Used Executables by Number of Users
- ◆ Software 08B: Users That Recently Used a Specified Executable
- ◆ Software 08C: Recently Used Executables by a Specified User

Hardware Inventory File Modification Requirements

Depending on how Configuration Manager was installed or upgraded, you may have to modify the files that define what properties are collected by hardware inventory; these are the sms_def.mof and configuration.mof files.

SMS_DEF.MOF MODIFICATION REQUIREMENTS

The following hardware inventory classes must be enabled in the sms_def.mof file to support the majority of Asset Intelligence reports. You can also enable these classes from the Configuration Manager console, as described in the "Configuring Asset Intelligence" section of this chapter:

- ♦ SMS_SystemConsoleUsage
- SMS_SystemConsoleUser
- SMS InstalledSoftware
- ◆ SMS_InstalledSoftwareMS
- SMS_AutoStartSoftware
- ◆ SMS_BrowserHelperObject
- SoftwareLicensingService
- SoftwareLicensingProduct
- ◆ Win32_USBDevice
- SMS_Processor

The Configuration Manager documentation from Microsoft also says that the following classes are required:

- ◆ SMS_InstalledExecutable
- SMS SoftwareShortcut

These classes are in fact optional, because they have no impact on any of the Asset Intelligence reports. In fact, enabling these classes is not recommended, because they may have an adverse effect on computer and network performance.

CONFIGURATION.MOF MODIFICATION REQUIREMENTS

CAL data collection must be enabled in the configuration.mof hardware inventory WMI data class CCM_CALTrackConfig to provide data for the Asset Intelligence Client Access License Reports. You can configure several parameters in that class to fine-tune CAL tracking to meet your organization's needs. The section "Enabling Asset Intelligence" details those parameters.

Site Maintenance Task Requirements

Two site maintenance tasks are associated with tracking CAL information, besides the modifications needed in the configuration.mof file:

- ◆ Delete Aged Client Access License Data Properties
- Summarize Client Access Weekly Usage Data

We will show how to configure these tasks later in the chapter.

DELETE AGED CLIENT ACCESS LICENSE DATA

This maintenance task is not necessary for data collection, but it should be used to help prevent the growth of unneeded data in the Configuration Manager database. This task will periodically delete aged CAL data from the site database when it is no longer needed.

SUMMARIZE CLIENT ACCESS LICENSE DATA

This maintenance task summarizes usage over a period of time and directly supports the Asset Intelligence license management report License 11A: Historical Client Access License (CAL) Utilization.

The CAL data that is collected from client hardware inventory reports represents a single computer at a single point in time. To get meaningful reports on CAL usage, it is necessary to gather that data into a summary that can be used for tracking usage trends over time.

Windows Event Log Settings

Four Asset Intelligence reports will display data gathered from the Windows security event logs on client computers. If the security event log is not set up properly, these reports will be empty even if the appropriate hardware inventory class has been enabled. We will discuss configuring these settings later in the chapter. The following reports require these collected events:

- Hardware 3A: Primary Computer Users
- Hardware 3B: Computers for a Specific Console User
- Hardware 4A: Shared (Multi-user) Computers
- Hardware 5A: Console Users on a Specific Computer

Elements of Asset Intelligence

Asset Intelligence enhances the inventory capabilities of Configuration Manager 2007 by extending hardware and software inventory and adding license management functionality, which was not robust in SMS 2003. The Asset Intelligence category now contains more than 50 reports that present this information in an easy-to-use format. Most reports link to more detailed reports that allow the administrator to query for general information and drill down to more detailed information as needed.

Asset Intelligence Catalog

The Configuration Manager 2007 Asset Intelligence catalog is a set of tables stored in the Configuration Manager database containing categorization and identification data for more than 300,000

software titles and versions that are divided into almost 100 families and almost 2,000 specific categories. These database tables are also used to manage hardware requirements for specific software titles and cataloged CPU properties information.

With Configuration Manager SP1, the Asset Intelligence catalog was enhanced to allow for software titles in use (both Microsoft and non-Microsoft software) to be manually imported. In addition, it now includes a large collection of known CPU properties, and the hardware requirements for software titles stored in the Asset Intelligence catalog have been updated. Also, it is now possible to edit the local Asset Intelligence catalog and to upload software title information to System Center Online for categorization.

WHAT IS SYSTEM CENTER ONLINE?

System Center Online is a "software as a service," hosted by Microsoft, that is an online management service aimed at the IT community. Some of the services that will be eventually hosted are antivirus, antispyware, system monitoring, backup/restore, policy management, and, in the case of Configuration Manager, asset inventory monitoring.

Asset Intelligence catalog updates containing newly released software and hardware definitions will be available for download periodically for bulk catalog updates, or the catalog can be dynamically updated by Microsoft SA customers using the Asset Intelligence synchronization point site system role.

SOFTWARE CATEGORIES

Administrators can view available software category information stored in the Asset Intelligence catalog by using the Asset Intelligence > Customize Catalog > Software Categories node in the Configuration Manager console.

These software categories are used to give broad categories of inventoried software titles and are also used as high-level groupings of more detailed software families. The Asset Intelligence catalog has many predefined software categories, and you can create user-defined categories to continue to define inventoried software as needed. For example, the predefined E-mail and Collaboration category includes applications such as Microsoft Outlook and Outlook Express. The validation state for software categories already defined is always validated, while custom category information added to the Asset Intelligence catalog is user-defined. Note that predefined software category information is read-only and can't be changed. User-defined software categories can be added, modified, or deleted by administrators. We will cover managing software categories later in the chapter in the section "Asset Intelligence Validation States."

SOFTWARE FAMILIES

Administrators can view available software family information stored in the Asset Intelligence catalog by using the Asset Intelligence > Customize Catalog > Software Families node in the Configuration Manager console.

Software families in Asset Intelligence are used to define inventoried software even further within software categories. For example, the Security software family is defined by the Security and Security Threat labels. Like software categories, predefined software families always have a validation state of validated, while custom software family information is user-defined. Also like software categories, predefined software family information can't be modified.

CUSTOM LABELS

Custom labels can be used to even further categorize inventoried software titles that are in the Asset Intelligence catalog. Administrators can use custom labels to create user-defined groups of software titles that share a common attribute. For example, a custom label could be called *bank software*, and that label would be used to identify inventoried bank software titles, which in turn can be used in a report to show all software that has that label. Custom labels will have no validation state since they are always created locally.

In the Configuration Manager console, you can view all the custom labels that you or another administrator has made in the Asset Intelligence catalog by choosing Asset Intelligence > Customize Catalog > Custom Labels.

INVENTORIED SOFTWARE TITLES

The Inventoried Software Titles node is located under the Asset Intelligence node in the Configuration Manager console. Administrators can look at inventoried software title information collected from Configuration Manager clients in this node and can even create up to three custom labels per inventoried software item to further use user-defined categorization.

Each software title shows the following information:

- ◆ Name of the software title
- Name of the software vendor
- Product version
- Assigned software category
- Assigned software family

All of this information except for software category and software family is read-only and can't be changed.

PROCESSOR PROPERTIES

You can use the Asset Intelligence > Processor Properties node to view processor property information about CPU types that are stored in the Asset Intelligence catalog. These processor properties are preloaded with the Asset Intelligence catalog and are not based on hardware inventory data. The following information is shown for each CPU that is listed:

- Name of the CPU
- Date of manufacture of the CPU
- Manufacturer of the CPU
- ◆ CPU brand ID
- CPU processing speed (in MHz)
- Whether the CPU is designed for mobile devices
- Amount of cache memory available for the CPU

This information can't be modified, and Microsoft promises that additional CPU information will be included in future Asset Intelligence updates from System Center Online.

HARDWARE REQUIREMENTS

With the Asset Intelligence > Hardware Requirements node, you can manage software title hardware requirements data that is stored in the Asset Intelligence catalog. The hardware requirements that are preloaded into the Asset Intelligence catalog are not based on inventoried software information but are included as part of the Asset Intelligence catalog. In addition to the default hardware requirements listed in this node, administrators can add new software title hardware requirements as needed to meet custom report requirements. The information that is displayed in this node includes the following:

- ◆ Name of the software title that hardware requirement is for
- Validation state for the hardware requirement (System Center Online requirements are always validated; custom hardware requirements are always user-defined)
- ♦ Minimum processor speed, in MHz, that is required for the software title
- ◆ Minimum RAM, in KB, that is required for the software title
- ♦ Minimum free disk space, in KB, that is required for the software title
- Minimum hard disk size, in KB, that the software title requires

As in other parts of the Asset Intelligence catalog, custom hardware requirements for software titles that aren't stored in the catalog can be modified, but the predefined information is read-only and can't be deleted.

Asset Intelligence Validation States

Asset Intelligence validation states show the source and current validation status of Asset Intelligence catalog information. They are outlined in Table 9.1, which is reproduced from the Configuration Manager documentation.

Asset Intelligence Synchronization Point

Configuration Manager SP1 added a new site system role for Asset Intelligence called the Asset Intelligence synchronization point. This site system role is used to connect to System Center Online over TCP port 443 so dynamic Asset Intelligence catalog updates can be managed.

This site role can be installed only on Configuration Manager 2007 SP1 central sites, and all of your Asset Intelligence catalog customization must be done on a Configuration Manager console that is connected to your central site. You must configure all the updates at the central site, but all Asset Intelligence catalog information is replicated to all child primary sites using the normal Configuration Manager site-to-site communication process.

The Asset Intelligence synchronization point can be used only by Microsoft SA customers who have registered with System Center Online and have received the required authentication certificate (*.pfx). This certificate file is required to install an Asset Intelligence synchronization point. (We will discuss connecting to System Center Online later in the chapter.)

Using the Asset Intelligence synchronization point, SA license customers can also request on-demand catalog synchronization with System Center Online or schedule automatic catalog synchronization, and they can upload uncategorized software titles to System Center Online for identification.

ABLE 9.1:	Asset Intelligence Validation Sates				
STATE	DEFINITION	Administrator Action	COMMENT		
Validated	Catalog item has been defined by System Center Online (SCO) researchers	None	This is the best state.		
User-defined	Catalog item has not been defined by SCO researchers	Customized the local catalog information	This state will be shown in Asset Intelligence reports.		
Pending	Catalog item has not been defined by SCO researchers but has been submitted for categorization	Requested categorization from SCO	The catalog item will remain in this state until SCO categorizes the item and the Asset Intelligence catalog is synchronized.		
Updateable	A user-defined catalog item has been categorized differently by SCO	Customized the local Asset Intelligence catalog to categorize an item as user-defined	The administrator can use the Software Details Conflict Resolution dialog box to choose which category to use.		
Uncategorized	Catalog item has not been defined by SCO; the item has not been submitted to SCO and has not been categorized by admin	None	Request categorization or customize local catalog. This is the base state of all unknown software.		

TABLE 9.1: Asset Intelligence Validation Sates

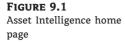
The Asset Intelligence Home Page

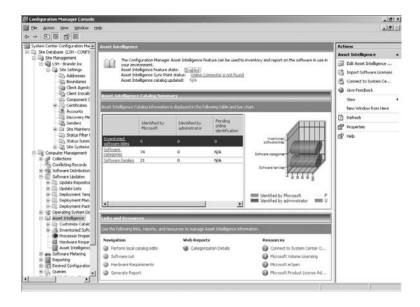
With Configuration Manager SP1, an Asset Intelligence home page was added to the Configuration Manager console; it's similar to home pages in some of the other features, such as software updates.

To display the Asset Intelligence home page, do the following in the Configuration Manager console: select System Center Configuration Manager > Site Database > site code > site name > Computer Management > Asset Intelligence. Figure 9.1 shows an example of the Asset Intelligence home page.

The Asset Intelligence home page is divided into the following sections:

- Asset Intelligence summary
- Asset Intelligence Catalog Summary section
- Asset Intelligence catalog synchronization summary
- Links and Resources section





ASSET INTELLIGENCE SUMMARY

This section displays the following information:

Asset Intelligence feature state Shows whether the Asset Intelligence feature has been enabled

System Center Online service connection status Specifies the connection status to System Center Online

Asset Intelligence catalog last updated Shows the time and date of the last Asset Intelligence catalog update

ASSET INTELLIGENCE CATALOG SUMMARY

This section displays the following information:

Asset Intelligence catalog summary information tables These display the Asset Intelligence catalog in summary table format with this information:

- ♦ Inventoried software titles
- Software categories
- ◆ Software families

Each of these are shown in one of the following states:

- Identified by Microsoft
- ◆ Identified by administrator
- Pending online identification

Asset Intelligence catalog summary information chart This displays an asset catalog summary in bar chart format, including the following information as percentages:

- Inventoried software titles
- Software categories
- ◆ Software families

These in turn are shown color coded for easier identification:

- ◆ Identified by Microsoft (green)
- Identified by administrator (blue)
- Pending online identification (yellow)
- Unidentified and not pending online identification (red)

Asset Intelligence catalog synchronization status summary This will be shown on the home page only if you have installed an Asset Intelligence synchronization point; this summary shows the following information:

Last download time The date and time of the last Asset Intelligence catalog synchronization with System Center Online

New software titles The number of new software titles added to the Asset Intelligence catalog during the last synchronization with System Center Online

New software categories The number of new software categories added to Asset Intelligence catalog during the last synchronization with System Center Online

New CPU types The number of new processor properties added to the Asset Intelligence catalog during the last synchronization with System Center Online

New conflicts The number of new categorization conflicts added to the Asset Intelligence catalog during the last synchronization with System Center Online

Pending categorization The number of new software titles from the Asset Intelligence catalog uploaded to System Center Online for categorization

Asset Intelligence Reports

To see the real power behind the Asset Intelligence feature, you have to examine the various Asset Intelligence reports that are provided with Configuration Manager right out of the box.

You can find the Asset Intelligence reports in the Configuration Manager console Reporting node, but there are also shortcuts to those reports under the Asset Intelligence ➤ Reporting node in the console.

The numbers of installed software and license information shown in Asset Intelligence reports may not be accurate; they may vary from the true number of software installed or licenses in use on your network because of complex dependencies and limitations in inventorying software license information for software titles installed in an enterprise environment. Therefore, you should not use Asset Intelligence reports as the sole source of deciding on purchasing software license compliance.

The following are example dependencies that are involved in inventorying installed software and licenses in an enterprise using Asset Intelligence that might affect the accuracy of the data:

Client hardware inventory dependency Asset Intelligence—installed software reports are based on data collected from SMS/Configuration Manager clients by extending hardware inventory to enable Asset Intelligence reporting. Because of this, Asset Intelligence reports will report data only from SMS/Configuration Manager clients that have completed a hardware inventory scan successfully and with the required Asset Intelligence WMI reporting class enabled. Also, since hardware inventory runs on a schedule that is set by the administrator, there may be a delay in data being reported that might affect the accuracy of Asset Intelligence reports at any given time.

Software packaging dependencies Because Asset Intelligence reports are based on installed software title data using standard Configuration Manager client hardware inventory processes, some of that data might not be collected properly if the software executables don't conform to standard installation processes or have been modified prior to installation.

Server role dependencies When using CAL reporting, it is important to remember that these reports were designed to provide visibility into the specific usage of products in specific scenarios, such as a Windows server hosting only one server role. In cases where a Windows server is hosting more than one role, this might cause inaccurate Asset Intelligence reports.

Location and usage Remember that Asset Intelligence reports were designed to report license usage, not how many licenses have been actually bought and for what purpose they are allowed to be used.

HARDWARE REPORTS

Asset Intelligence hardware reports provide information about hardware assets in your organization, such as a computer's age and its ability to handle a software upgrade. Some reports are based on information collected from the System Security Event Log, so you should clear that log if a computer is assigned to another user. The following hardware Asset Intelligence reports are available:

Hardware 01A: Summary of Computers in a Specific Collection

Hardware 02A: Estimated Computer Age by Ranges Within a Collection

Hardware 02B: Computers Within an Age Range Within a Collection

Hardware 03A: Primary Computer Users

Hardware 03B Computers for a Specific Primary Console User

Hardware 04A: Shared (Multi-user) Computers

Hardware 05A: Console Users on a Specific Computer

Hardware 06A: Computers for Which Console Users Could Not Be Determined

Hardware 07A: USB Devices by Manufacturer

Hardware 07B: USB Devices by Manufacturer and Description

Hardware 07C: Computers with a Specific USB Device

Hardware 07D: USB Devices on a Specific Computer

Hardware 08A: Hardware That Is Not Ready for a Software Upgrade

Hardware 09A: Search for Computers

Hardware 10A: Computers That Have Changed Within a Specified Collection

Hardware 10B: Changes on a Specified Computer Within a Time Range

Hardware 10C: Changes in a Specified Class on a Specified Computer



PLANNING FOR A SOFTWARE UPGRADE

You get word from your manager that the department responsible for all the company training manuals is working on updating many of the manuals because of some new federal regulations. They are making these updates with a new version of the Adobe Acrobat software, and there is a possibility that you might have to deploy Acrobat Reader 8 so that employees will be able to read the updated manuals properly.

The company is also in the middle of a hardware refresh, so your manager is concerned that there may be computers on the network that do not have the necessary hardware requirements to run Adobe Reader 8 properly, so she wants to use Configuration Manager to generate a list of those computers if there are any.

Hearing this, you are glad that you have already enabled Asset Intelligence, because there is a specific report for just this scenario. To meet your manager's request, just go to the report Hardware 08A: Hardware That Is Not Ready for a Software Upgrade. Since you are concerned with user computers in this instance, select the collection All Workstations or Professional Systems for the Collection field. The Asset Intelligence knowledge base, which is part of the Configuration Manager database, already has information about Adobe Reader 8, so select that for the Product field.

After you run the report, you can provide that link to your manager so she can either print it or export it into Excel for her own use.

SOFTWARE REPORTS

Software Asset Intelligence reports provide information about software families, categories, and specific software titles installed on computers within your organization. The following software Asset Intelligence reports are available:

Software 01A: Summary of Installed Software in a Specific Collection

Software 02A: Software Families

Software 02B: Software Categories with a Family Software 02C: Software by Category and Family

Software 02D: Computers with a Specific Software Product

Software 02E: Installed Software on a Specific Computer

Software 03A: Uncategorized Software

Software 04A: Auto-start Software

Software 04B: Computers with a Specific Auto-start Software

Software 04C: Auto-start Software on a Specific Computer

Software 05A: Browser Helper Objects

Software 05B: Computers with a Specific Browser Helper Object Software 05C: Browser Helper Objects on a Specific Computer

Software 06A: Search for Installed Software

Software 07A: Recently Used Executables by Number of Computers

Software 07B: Computers That Recently Used a Specified Executable

Software 07C: Recently Used Executables on a Specific Computer

Software 08A: Recently Used Executables by Number of Users

Software 08B: Users That Recently Used a Specified Executable

Software 08C: Recently Used Executables by a Specified User

Software 09A: Infrequently Used Software (SP1)

Software 09B: Computers with Infrequently Used Software Installed (SP1)

Software 10A: Software Titles with Specific, Multiple Custom Labels Defined (SP1)

Software 10B: Computers with a Specific Custom Label Software Title Installed (SP1)

Software 11A: Software Titles with a Specific Custom Label Defined (SP1)

Software 12A: Software Titles Without a Custom Label (SP1)

LICENSE MANAGEMENT REPORTS

There are nine new license management reports in Configuration Manager 2007, now providing the ability to track CALs as well as the volume license reports from SMS 2003. The following License Management Asset Intelligence reports are available:

License 01A: Microsoft License Ledger for Microsoft License Statements

License 01B: Microsoft License Ledger Item by Sales Channel

License 01C: Computers with a Specific Microsoft License Ledger Item and Sales Channel

License 01D: Microsoft License Ledger Products on a Specific Computer

License 02A: Count of Licenses Nearing Expiration by Time Ranges

License 02B: Computers with Licenses Nearing Expiration

License 02C: License Information on a Specific Computer

License 03A: Count of Licenses by License Status

License 03B: Computers with a Specific License Status

License 04A: Count of Products Managed by Software Licensing Service

License 04B: Computers with a Specific Product Managed by Software Licensing Service

License 05A: Computers Providing Key Management Service

License 06A: Processor Counts for Per-Processor Licensed Products

License 07A: Client Access License (CAL) Usage: Summary

License 08A: Client Access License (CAL) Usage: Product Specific

License 08B: Client Access License (CAL) Utilization Details: Product Specific

License 09A: List of Users Utilizing Windows Server Client Access Licenses (CAL)

License 09B: Client Access License (CAL) Utilization Details for a Specific User

License 10A: List of Devices Utilizing Windows Server Client Access Licenses (CAL)

License 10B: Client Access License (CAL) Utilization Details for a Specific Device

License 11A: Historical Client Access License (CAL) Utilization

License 12A: Servers from which Client Access License (CAL) Usage Data Cannot Be Collected

License 13A: Core Client Access License (Core CAL) Usage Summary

License 14A: Microsoft Volume Licensing Reconciliation Report

License 14B: List of Microsoft Software Inventory Not Found in MVLS

License 15B: Third Party Reconciliation Report

Configuring Asset Intelligence

If you upgraded to Configuration Manager from SMS 2003 SP3 and were using Asset Management, then Asset Intelligence data collection is already enabled on your Configuration Manager site, and you don't have to worry about this section. Keep in mind, however, that the Asset Management category in SMS 2003 has been renamed to Asset Intelligence. When you upgrade to Configuration Manager, the existing Asset Management reports will be deleted, and the Asset Intelligence reports will be added in their place, deleting any modifications that you made to the stock reports and more than likely any custom reports that you added to that category as well.

If you installed Configuration Manager from scratch, you will find that Asset Intelligence is not enabled by default. Depending on what data that you want information on, you will have to edit the Configuration Manager MOF files and make sure that certain client agents are enabled, which we will go over in the following sections.

Enabling Asset Intelligence

To collect data for the hardware and software reports in Asset Intelligence, you first need to enable the Hardware Inventory Client Agent. You'll see how to do that in Chapter 10.

The classes that are used for the Hardware and Software Inventory reports include the following:

- SMS_SystemConsoleUsage
- ◆ SMS_SystemConsoleUser
- SMS_InstalledSoftware
- SMS_InstalledSoftwareMS

- SMS AutoStartSoftware
- ◆ SMS_BrowserHelperObject
- ◆ SoftwareLicensingService
- ◆ SoftwareLicensingProduct
- ♦ Win32_USBDevice
- ♦ SMS_Processor

To enable one or all of these classes in Configuration Manager RTM, you have to open the sms_def.mof file in Notepad and search for each of the names, and change the SMS_Report item in each class from False to True. You can find this file, as well as the configuration.mof file, in the following location:

Location where ConfigMgr is installed/Inboxes/clifiles.src/hinv Editing the sms def.mof file like this is discussed in more detail in Chapter 10.

With Asset Intelligence in Configuration Manager SP1 or higher, you can enable these classes right from the Configuration Manager console. Go to the Asset Intelligence home page, and click the Edit Asset Intelligence Reporting Class Settings option in the Actions pane to the right of the home page. Figure 9.2 shows the dialog box that opens.

FIGURE 9.2 Asset Intelligence Reporting Class Settings dialog box



After you do that, it could take up to a few days for these changes to take full effect, depending on your Configuration Manager hierarchy and how often you have the Hardware Inventory Client Agent set to run inventory.

Configuring Collecting Client Access License Data

As mentioned earlier, some new CAL reports have been added to the existing License Ledger reports. These reports complete the ability to compare license usage with Microsoft License Statements.

To be able to use those reports, however, you will have to edit the WMI data class CCM_CALTrackConfig in the configuration.mof file. That class contains several variables defining the way that CAL data is collected; you can set these variables in the configuration.mof file, as shown in Figure 9.3.

FIGURE 9.3
The configuration.mof file

```
| Set | Set
```

The CALCollectionType parameter controls whether CALs will be tracked for devices, users, or both. To enable CAL data collection in the first place, you have to change the value from 0 to one of the values in Table 9.2.

TABLE 9.2: Values for CALCollectionType

VALUE	Meaning
0	Data collection disabled
1	User CAL collection only
2	Device CAL collection only
3	All CAL collection enabled

To enable CAL collection for the rest of your hierarchy, you will have to make the same changes to the rest of your sites.

The CALCollectionFrequencyDays parameter controls the frequency, in days, of the CAL data collection. You can set this to any value from 0 and 90, with a default of 7. A single server can be accessed by thousands of users and devices a day, which will create a record in the Configuration Manager database and could cause problems with network traffic if it is set to gather

this data too frequently. Gathering this data on a weekly basis is sufficient for tracking CAL information. If you set this to 0, polling defaults control to the CALCollectionFrequencyMinutes parameter.

The CALCollectionFrequencyMinutes parameter controls the CAL collection frequency based on minutes. You can set this value from 0 to 1440, with no default value. If the value is set to 0, then polling frequency defaults to CALCollectionFrequencyDays. We don't recommend using this setting for setting CAL collection frequency, except for in an isolated lab scenario, since polling for CAL information too frequently can cause a large amount of network traffic.

The CALCollectionTimeWindow parameter controls how often CAL licensing can be reassigned. The current Microsoft licensing model allows for CALs to be reassigned every 90 days, so this value shouldn't be modified. If Microsoft changes its licensing model later, you can adjust this value according to the new value to any number from 1 to 365.

The CALSupportedWindowsVersions parameter lists the operating system versions that are polled for client access information to limit polling to servers. Don't modify this parameter, or you will get inaccurate CAL counts.

SITE MAINTENANCE TASKS FOR CAL LICENSING COLLECTION

Two site maintenance tasks go with CAL licensing:

Summarize Client Access License Weekly Usage Data This task makes summaries of usage over time and directly feeds the License 11A: Historical Client Access License (CAL) Utilization report. This is necessary to have meaningful reports on data so you can track usage trends over time.

Delete Aged Client Access License Data This task isn't needed for data collection or feeding reports but should be enabled to keep unneeded data out of the Configuration Manager database by purging aged CAL data.

INSTALLING AN ASSET INTELLIGENCE SYNCHRONIZATION POINT

As discussed earlier in the chapter, the Asset Intelligence Synchronization point role is used to connect Configuration Manager SP1 (or higher) sites to System Center Online to synchronize Asset Intelligence catalog information. You can install this role only on a site system located in the central site of a Configuration Manager SP1 hierarchy, and you'll require Internet access to synchronize with System Center Online on TCP port 443. The Asset Intelligence Synchronization point can also upload custom software title information to System Center Online for categorization. All information uploaded to System Center Online will be treated as public information by Microsoft, so you should be sure that your custom information does not contain any sensitive information.

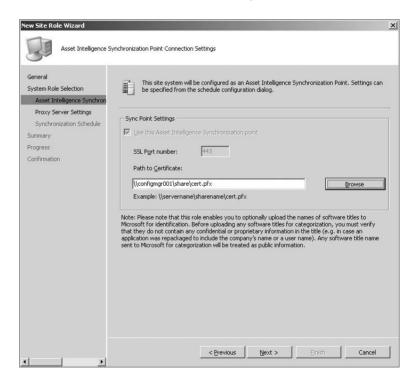
To install the Asset Intelligence Synchronization point, you will need a System Center Online (SCO) authentication certificate (*.pfx), which can be acquired only by SA license customers. (For more information on Software Assurance, check out the SA website at www.microsoft.com/licensing/sa/default.mspx.) Before you begin the installation of the Asset Intelligence synchronization point, make sure that all of the following are true:

- You have a valid SCO authentication certificate.
- Asset Intelligence Synchronization point is available on a shared network folder accessible to the server where you will be running the New Site Role Wizard.
- Asset Intelligence Synchronization point stays in that location until the Asset Intelligence Synchronization point has done its first synchronization with System Center Online.

To install an Asset Intelligence synchronization point, follow these steps:

- **1.** In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ site code ➤ site name ➤ Site Settings ➤ Site Systems.
- **2.** Right-click the name of the site system on which you want to install the Asset Intelligence synchronization point role, and then click New Roles to start the New Site Role Wizard.
- **3.** As you have done with other Configuration Manager wizards covered in this book, verify the site system settings on the General page, and click Next.
- On the System Role Selection page, select the Asset Intelligence Synchronization Point box, and then click Next.
- **5.** On the Asset Intelligence Synchronization Point Connection Settings page, set the path to the SCO authentication certificate (*.pfx) file, as shown in Figure 9.4, and click Next.

FIGURE 9.4
Asset Intelligence Synchronization Point Connection Settings page



- **6.** On the Proxy Server Settings page, configure the settings for the proxy server if needed.
- 7. On the Synchronization Point Schedule page, you can set whether to set up synchronization on a simple or custom schedule, as you've seen in other Configuration Manager options.
- **8.** On the Summary page of the wizard, review the settings you have specified to make sure they are correct. If you need to make any changes, click the Previous button. Otherwise, click Next to finish the rest of the configuration if necessary.

The Bottom Line

Enable Asset Intelligence. If you installed Configuration Manager from scratch, you will find that Asset Intelligence is not enabled by default. Depending on the data that you want information on, you will have to edit the Configuration Manager MOF files and make sure that certain client agents are enabled.

Master It What are the classes in the sms_def.mof file that you have to enable to use Asset Intelligence?

Enable Client Access License tracking. There are new CAL reports that have been added to the existing License Ledger reports. These reports complete the ability to compare license usage with Microsoft License Statements.

To be able to use those reports, however, you will have to edit the singleton class CCM_CALTrackConfig in the configuration.mof file. That section of the file contains several variables controlling the way that CAL data is collected.

Master It What does the CALCollectionTimeWindow parameter in the configuration.mof file set?

Configure the Asset Intelligence Synchronization Point. The Asset Intelligence Synchronization Point is used to connect to System Center Online to synchronize Asset Intelligence catalog information and get periodic updates.

Master It What are the two things that are required in order to use an Asset Intelligence synchronization point?

Chapter 10

Inventory and Software Metering

Out of all of the capabilities of Configuration Manager 2007, inventory is considered a "core" feature; it is one that, by itself, has made Configuration Manager and its predecessors a very useful product since the days of SMS 1.0.

Configuration Manager has the ability to inventory the hardware and software in client computers. Hardware inventory can gather information from your systems such as the processor, computer manufacturer, and amount of installed memory. Software inventory can gather lists of file types and their versions installed on your computers, with EXE files being the default. Combine this with the extensive information in the Asset Intelligence knowledge base covered in the preceding chapter, and you can use Configuration Manager to really get a handle on what kind of software is being used in your environment. Inventory can be considered the backbone of Configuration Manager; you can run it without enabling inventory, but you really wouldn't be able to do much, since other features, such as software metering, require it.

Software metering, the second major topic in this chapter, allows you to collect information on software usage to assist in managing software purchases and licensing. With this feature, you can report on the software that is being used in your environment and which users are running particular programs. You can also find software that is installed but isn't being used, and you can report on software license requirements and other items related to license management.

In this chapter, you will learn how to do the following:

- Configure and manage Software Inventory
- Configure and manage Hardware Inventory
- Configure and manage Software Metering

Inventory in Configuration Manager 2007

To use the inventory feature in Configuration Manager 2007, you need to make sure its two client agents, for hardware and software, are enabled (which they are by default). These agent settings configured on a site-wide basis.

When the Hardware Inventory Client Agent is enabled for a Configuration Manager site, hardware inventory data gives you system information about each of your clients, including details such as disk space, video card type, memory installed, and operating system.

When the Software Inventory Client Agent is enabled, you can gather information from your clients on the software installed, file types, and the versions of software. With this agent, you can also collect files up to a certain size, not just details about them, from clients. All you need to do is set the files or file types for inventory or collection, and the agent does the rest.

Inventory agents can also create an inventory report based on the client's information and send it to the client's management point. The management point then collects data from many clients and sends that data to a Configuration Manager site server, where it is imported into the site database. You can use several methods in Configuration Manager to use that information in your organization:

- You can create queries that target computers based on their hardware configuration or installed software. You can use these queries to be proactive in preventing problems such as low hard disk space.
- You can create queries that show computers that don't have your organization's standard
 antivirus program installed in order to make a collection that can be a target for deploying
 that software to the computers that have the hardware to support it.
- You can create reports showing hardware configuration and software installations that management can use to improve the current computer environment.
- You can provide Resource Explorer or reports on individual computers that your PC support department can use to remotely troubleshoot problems.

Whenever either inventory client scans a client computer, the first inventory is always a full report on all of the hardware and software resources present on the client. After that, subsequent scans, which are run on a schedule you define, will show only *delta* inventory information, identifying what has changed.

Delta inventory reports, for both inventory agents, are processed in the order they are received at the Configuration Manager site server. If for some reason a delta inventory is received from a client that is not in the database (such as a reimaged or new client, for example), is out of order, or is missing, then the site server will throw out the delta inventory and ask for a full inventory from that client the next time a scheduled scan is run.

Configuration Manager provides only limited support for computers that can boot up two or more operating systems. Configuration Manager clients can be discovered in multiple boot states, and the clients can be installed on each boot state. Inventory that is collected from these computers, however, will only be from the operating system that was running when the inventory scans were run.

Collecting Hardware Inventory

Hardware inventory collects data from clients by querying several data stores of information that are on computers, such as the registry and Windows Management Information (WMI). The Hardware Inventory Client Agent doesn't query all possible WMI classes, but it does pull information from about 1,500 hardware properties and 100 different WMI classes by default. You can customize the information that is gathered from hardware inventory according to your organization's needs; we will provide some details on that later in the chapter.

The initial full hardware inventory on the client is based on reporting requirements set up in each Configuration Manager site's sms_def.mof file that is stored on each primary site. This definition sets the baseline for all other inventory scans, and you will need to ensure that this file is the same for all primary sites in your Configuration Manager site hierarchy to keep inventory consistent and to keep errors from being reported on inventory classes that don't exist.

Other inventory scans are done on the schedule you set up in the Hardware Inventory Client Agent properties. (Later in the chapter you'll create a complete sample Hardware Inventory Client Agent configuration, including a schedule.) Unless there is a problem with the client, only

delta inventories will be collected after the first baseline inventory that was run when the computer first had the Configuration Manager client installed. This greatly decreases the network traffic required by client inventory reporting because deltas are usually only a small percentage of the size of a full inventory from a client. With every hardware inventory collection done on a client, Configuration Manager updates the site database with the current inventory while keeping a history of the previous information. You can view the current and historical inventory information in queries, reports, and Resource Explorer.

Hardware inventory will also collect certain basic information about a client's installed software. This information is gathered from the registry, most notably from Add Or Remove Programs. By using the software inventory, however, you can get larger and much more detailed information about the software that is present on client computers.

WHAT DEFINES HARDWARE INVENTORY?

Configuration Manager gathers information about clients based on the contents of two managed object format (MOF) files stored on the primary site server in the <Folder where Configuration Manager is installed>\inboxes\clifiles.src\hwinv folder. The two MOF files used by hardware inventory are configuration.mof and sms_def.mof.

The configuration.mof File

The configuration.mof file defines the data classes to be inventoried by the Hardware Inventory Client Agent. Data classes can be created to inventory existing or custom WMI repository data classes or registry keys found on clients.

This file also defines and registers the WMI providers used to access computer information during hardware inventory. Registering providers defines the type of provider to be used and the classes that the provider will support. WMI can access only registered providers, so that applies to the Hardware Inventory Client Agent as well. The configuration.mof file can't be used to register new providers for clients. New or custom providers must be sent to clients to be compiled manually before they can be added to hardware inventory.

When Configuration Manager clients request computer policies as part of their policy polling interval, the configuration.mof file is part of the policy that clients download and compile. When you add, modify, or delete data classes from the configuration.mof file, clients will automatically compile those changes the next time the client compiles a computer policy that it receives.

Later in the chapter you'll get hands-on practice in modifying configuration.mof to extend the information collected in hardware inventory.

The sms_def.mof File

The sms_def.mof file defines the reporting classes used by the Hardware Inventory Client Agent to define whether specific client data class information is reported. Reporting classes are based on the WMI data classes that are on clients by default or have been added after the configuration.mof file has been modified.

This reporting class information in the sms_def.mof file is converted to a reporting policy that is downloaded to clients as part of their computer policy polling download. After the client is done compiling the new reporting policy, the reporting information is stored in the client WMI repository in the InventoryDataItem class of the Root\CCM\Policy\Machine WMI namespace. Unlike the configuration.mof file, the sms_def.mof file is never sent to clients directly. Only the policy generated by the sms_def.mof file is actually compiled by Configuration Manager clients.

Later in the chapter you'll get hands-on practice in modifying sms_def.mof to extend the information collected in hardware inventory.

Default Hardware Inventory Reporting Classes

The sms_def.mof file already has some reporting classes enabled by default. These default classes depend on what version of Configuration Manager and Service Pack you have installed and on whether you have enabled classes for Asset Intelligence. Here is an example of the Hardware Inventory data classes that are enabled by default in Configuration Manager R2 with Asset Intelligence classes enabled. This list can change at any time depending on hotfixes or Service Packs installed or features enabled.

- ◆ Add Or Remove Programs
- ◆ AutoStart Software
- Browser Helper Object
- CDROM Drive
- Computer System
- Desktop Monitor
- Disk Drives
- Disk Partitions
- ◆ IDE Controller
- Installed Software MS
- Logical Disk
- Memory
- Motherboard
- Network Adapter
- Network Adapter Configuration
- Network Client
- Operating System
- Parallel Port
- ◆ PC BIOS
- ♦ PNP Device Driver
- ◆ Processor
- Recently Used Applications
- SCSI Controller
- Services
- SMS Advanced Client SSL Configurations
- SMS Advanced Client State
- System

- System Console Usage
- System Console Usage
- ◆ System Console User
- ♦ System Devices
- System Enclosure
- USB Controller
- Video Controller
- ◆ Virtual Machine
- Windows Update Agent Version
- Workstation Status

Each one of these reporting classes has certain criteria enabled; these represent the actual data classes that are being collected. Some reporting classes might have all their data classes being captured or only some of them. The best way to get a handle on what is being actually collected by hardware inventory is to read the sms_def.mof file so you can see what is actually enabled, which will allow you to determine whether you need to collect any further information.

THE ROLE OF MIF FILES IN HARDWARE INVENTORY

Management information format (MIF) files can be used to extend hardware inventory information that is collected from clients. The type of information that can be collected by MIF files can be just about anything, depending on how the MIF file is structured. During a hardware inventory cycle, the information in a MIF file is added to the client inventory report and stored in the Configuration Manager site database, where it can be used just like default client inventory data. The two types of MIF files that can be used to extend hardware inventory in this way are NOIDMIF and IDMIF.

By default, NOIDMIF and IDMIF file information is not inventoried by Configuration Manager. For this information to be added to hardware inventory, you must enable one or both file types in the Hardware Inventory Client Agent settings. When you do, Configuration Manager creates new tables or modifies existing tables in the site database to add the properties in NOIDMIF and IDMIF files. NOIDMIF and IDMIF files are not validated, so they can be used to alter tables that you don't want altered. Doing this runs the risk that valid data could be overwritten by invalid data or large amounts of data could be imported into the Configuration Manager database, which would cause delays in all Configuration Manager functions. To lower the risk of this happening, use MIF collection only when it is absolutely necessary.

Later in the chapter, you'll see how to change the location of MIF files from the default.

More on NOIDMIF Files

NOIDMIF files are the standard MIF files that are used in Configuration Manager Hardware Inventory. NOIDMIF files do not contain a unique identifier for the data they contain, and hardware inventory automatically associates the NOIDMIF information with the client that it was found on. NOIDMIF files are not sent to the site server during a client hardware inventory cycle, but their data is added to the client inventory report itself.

If the classes in the NOIDMIF file don't exist in the Configuration Manager database, the new inventory class tables are created in the Configuration Manager site database to store the new

inventory information. As long as the NOIDMIF file is present on the client, the inventoried data from the NOIDMIF files will be updated in the Configuration Manager database. If the NOIDMIF file is removed, all the classes and properties relating to it are removed from the inventory of that client in the database. For NOIDMIF information to be pulled from a client, the NOIDMIF file must be put here: <code>%WINDIR%\System32\CCM\Inventory\Noidmifs</code>.

More on IDMIF Files

IDMIF files are custom MIF files that contain a unique ID and are not attached to the client that they are collected from. IDMIF files can be used to collect inventory data about devices that are not Configuration Manager clients, such as a shared network printer, an external hard drive, a copy machine, or other equipment that may not be attached to a client computer.

When you enable the IDMIF collection on your Configuration Manager site, IDMIF files are collected only if they are within the size limit that you set in the Hardware Inventory Client Agent properties. Depending on the maximum custom MIF size that you set of each site, IDMIF collection may cause increased network bandwidth usage during client inventory, which should be considered before you enable IDMIF collection.

Differences Between NOIDMIF and IDMIF Files

IDMIF files are in most ways the same as NOIDMIF files. Both types have key properties that must be unique. Any class that has more than one instance must at least have one key property defined, or instances will overwrite previous instances. They differ in the following ways:

- ◆ IDMIF files must have a delta header that gives architecture and a unique ID. NOIDMIF files are given a delta header automatically when processed by the client.
- IDMIF files must have a top-level group with the same class as the architecture being added or changed, and the class must have at least one property.
- Removing an IDMIF file from a client doesn't cause any data to be deleted from the Configuration Manager database.
- IDMIF files aren't added to a client's inventory, and the files themselves are sent across the network to be processed by a site server.

Collecting Software Inventory

When you enable software inventory in Configuration Manager, the Software Inventory Client Agent collects software inventory data directly from files (such as the default .exe files) by gathering data from the file's header information. Unknown files (files that don't have any detailed information in their file headers) can also be inventoried. You can also have Configuration Manager actually collect files you configure under a certain size. Both software inventory and collected file information can be viewed in Resource Explorer, which we will discuss later in the chapter.

You can also inventory encrypted and compressed files with the Software Inventory Client Agent, but this will usually cause software inventory to run much slower because of the extra processing imposed on the client computer. When you inventory an encrypted file, an unencrypted copy of the file must be made so its information can be scanned. If antivirus software is running at the same time, it will show that the Software Inventory Client Agent is opening the files that are being scanned and then scanning them again to make sure they aren't infected by a virus.

Software inventory can use a considerable amount of network capacity, depending on the number of Configuration Manager clients, how frequently you schedule software inventory, and

the size of the files you collect (if any, which we wouldn't recommend anyway). If you think that software inventory will cause problems with your network, schedule it to run after business hours.

Later in the chapter you'll create a complete sample software inventory client agent configuration, including a schedule.

MORE ABOUT FILE COLLECTION

When a file is selected for collection, the software inventory client agent will search for that file when a software inventory scan runs on each client in the Configuration Management site. If the software inventory client agent finds a file that should be collected, then the file is attached to the inventory report and sent to the site server.

The site server keeps the five most recently changed versions of the collected files and stores them in the <Configuration Manager installation directory>\Inboxes\Sinv.box\Filecol directory. If a file has not changed since the last software inventory was collected, the file will not be collected again. Files larger than 20MB are not collected by Configuration Manager software inventory file collection even if they are defined in the file collection settings.

This feature of Configuration Manager can greatly affect network bandwidth, as well as cause other problems. With this in mind, we recommend not using it in any circumstance.

DISPLAY NAMES FOR SOFTWARE INVENTORIED PRODUCTS

During a software inventory cycle, the Configuration Manager 2007 Software Inventory Client Agent gets information from the file headers of files installed on clients. That information, including the names of the companies that made the files and the names of the files (or software products) themselves, is also inventoried. After the data is collected, you can view the information with Resource Explorer.

Because company and product names are retrieved from the file header information, any mismatches in the way these names are entered in the header information will also appear in the Configuration Manager database. These mismatches make it difficult to read and query against software inventory information since the data will appear to be under multiple company or software product names instead of a single name.

To help with this issue, you can set display names for inventoried products on the Inventoried Names tab of the Software Inventory Client Agent tab. For example, you can change variations of a company name to a single display name, as shown in Table 10.1.

TABLE 10.1:	Examples of	Mismatched	Names from	Software Inventory
-------------	-------------	------------	------------	--------------------

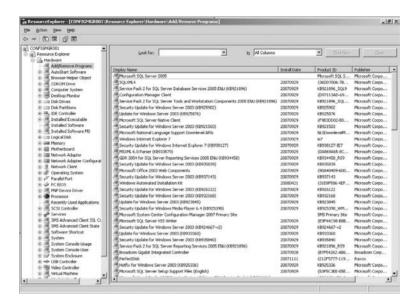
CHANGE THIS NAME:	To This One:
Wayne Enterprises	Wayne Enterprises, Inc.
Wayne Enterprises Inc	Wayne Enterprises, Inc.
Wayne enterprises	Wayne Enterprises, Inc.

After you have made this change, refresh the view of software inventory in Resource Explorer, and you will see the company name "Wayne Enterprises, Inc." instead of the three variations. You will also see this new company name when you make and run queries. Doing this doesn't actually change the names in the file header information of the files installed on clients; it changes the names in the Configuration Manager site database.

Using Resource Explorer to View Inventory

When hardware and software inventory is collected from clients, it can be viewed by Resource Explorer. When you start Resource Explorer, a new MMC console opens, as shown in Figure 10.1.

FIGURE 10.1
Resource Explorer



This displays the information collected from clients by hardware inventory and software inventory. The contents of the Resource Explorer details pane on the right will vary depending on what node is selected on the left pane in the console tree. You can use Resource Explorer to view client hardware, hardware history, and software inventory.

If a resource is a Configuration Manager client and if you are collecting hardware inventory at your site, the information displayed for that resource will be a list of the hardware installed on the client and other details. If you are collecting software inventory, then you will see a list of installed software on the client. If the resource isn't a Configuration Manager client, then no information will be displayed, since no inventory will be collected from that client.

You can start Resource Explorer to view a single client's inventory from the Configuration Manager console or from a command line.

OPENING RESOURCE EXPLORER FROM THE CONFIGURATION MANAGER CONSOLE

To open Resource Explorer from the Configuration Manager console, follow these steps (Read permission on collections is required):

- In the Configuration Manager console, select System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Collections.
- Open Collections so you can see more details, and find the collection with the client that you want to view.
- **3.** Once you have found the client you want, right-click it.
- 4. Then click All Tasks and then Start Resource Explorer.

OPENING RESOURCE EXPLORER FROM THE COMMAND LINE

To open Resource Explorer from the command line with a specific resource identifier, enter the following all on one line:

```
<console path>\resourceexplorer.msc
-s -sms:ResourceID=<n> -sms:Connection=<namespace path>
```

These are the command-line switches for resource identifiers:

⟨console path⟩ This is the full path to resourceexplorer.msc. If you start

this from the Run dialog box, you will have to enter the full path to resourceexplorer.msc. By default this is the

Configuration Manager install location.

<n> This is the resource ID of the Configuration Manager client

for which you want to display information.

<namespace path> This is the path to the WMI namespace that contains your

client data (\\<site server name>\root\sms\site_<site</pre>

code>).

To open Resource Explorer from the command line with a specific computer name, enter the following all on one line:

```
<console path>\resourceexplorer.msc -s -sms:ResExplrQuery=
"SELECT ResourceID FROM SMS_R_SYSTEM WHERE Name = "<computer name>"
-sms:Connection=<namespace path>
```

These are the command-line switches for specific computer names:

<console path> This is the full path to resourceexplorer.msc. If you start

this from the Run dialog box, you will have to enter the full path to resourceexplorer.msc. By default this is the

Configuration Manager install location.

<computer name>
This is the name of the computer for which Resource

Explorer will attempt to display inventory data.

<namespace path> This is the path to the WMI namespace that contains your

client data (\\<site server name>\root\sms\site_<site</pre>

code>).

Scheduling Inventory

The Hardware Inventory Client Agent and Software Inventory Client Agent each collect inventory according to a schedule that is set in the client agent properties in the Configuration Manager console for each site; the schedule is set on a site-wide basis. Table 10.2 gives a simple rundown of scheduling options for each inventory agent.

By default, both hardware and software inventory schedules are set to run every seven days. If a client is not running when an inventory is schedule to run, it will run the inventory the next time the client is started.

TA	BLE 10.2: In	nventory Scheduling Options
	Түре	DESCRIPTION
	Simple schedule	An interval between inventory cycles, such as every 24 hours or every 6 weeks
	Custom schedule	A start time and an interval for inventory collection, such as every Monday or the first Tuesday of every month

The simple schedule doesn't give you as much flexibility as custom scheduling does; however, the simple schedule usually causes less network traffic because the time interval between each client's inventory cycle is based on the time that the Configuration Manager client was installed, and when the first policies are retrieved, for every client. When you use a custom schedule, all the clients will begin inventory cycles at exactly the same time.

Since software inventory is more resource-intensive on clients than hardware inventory, you might consider not running software inventory as often as you do hardware inventory, depending on your organization's needs. For example, if your organization has locked down user rights on workstations, then the software that is installed on them should not change very frequently, so you can set software inventory cycles for every few days or once a week.

When you change an inventory collection schedule on the Configuration Manager site server, this will update the client computer policies downloaded and compiled by clients according to their regular client policy polling interval. When the client inventory agent detects a change in schedule, it will make a delta inventory file. The next inventory cycle will run according to the new schedule.

Configuration Manager also keeps historical inventory records for the number of days set in the Delete Aged Inventory History site maintenance task, which has a default setting of 90 days.

Configuring Inventory

Now that we have discussed the inventory process, its components, and its capabilities, you are ready to configure the inventory function to fit your company's needs.

CONFIGURING HARDWARE INVENTORY FOR A CONFIGURATION MANAGER SITE

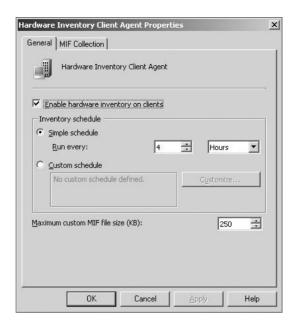
To configure hardware inventory for a site, you must have the Modify permission for the site. Then follow these steps:

- In the Configuration Manager console, select System Center Configuration Manager ➤ Site
 Database ➤ Site Management ➤ site code ➤ site name ➤ Site Settings ➤ Client Agents.
- 2. In the left pane, right-click Hardware Inventory Client Agent, and then click Properties.

First you will see the General tab, as in Figure 10.2. The settings include the following:

Enable Hardware Inventory On Clients Select or deselect this box to enable (default) or disable hardware inventory for the entire site.

FIGURE 10.2
General tab of the Hardware Inventory Client
Agent settings



Inventory Schedule Either select a simple schedule or define a custom schedule:

Simple Schedule This schedules hardware inventory to run on a single, specific interval for all clients in the site. By default, this option is enabled and set for seven days. For any other setting, use the Run Every field, and enter the number and type of time units (minutes, hours, days) in the simple schedule. This setting can be from 1 to 60 minutes, 1 to 24 hours, or 1 to 31 days.

Custom Schedule Click Customize to open the Custom Schedule dialog box and set the hardware inventory schedule. This gives you the ability to schedule the first start date and time for inventory to run on clients. Once the start time for inventory has passed, all future inventories will recur on the schedule that you set on all clients at the same time. The custom schedule can be set to run weekly, to run monthly, or to run on a custom interval, with the following criteria:

- Custom weekly schedule can run from one to four weeks on the day of the week you set.
- ◆ Custom monthly schedules can run from 1 to 12 months on either a specific day of the week from 1 to 31; the last day of each month; or the first, second, third, fourth, or last selected day of the week for each month.
- ◆ Custom schedules can also be set on a custom interval of either 1 to 31 days, 1 to 23 hours, or 1 to 59 minutes.

Maximum Custom MIF File Size (KB) This is the maximum size, in kilobytes, allowed for each custom MIF file that will be collected from a client during a hardware inventory cycle. You can set the size from 1KB to 5,000KB; and the default value is 250KB. If a custom MIF is

larger than the maximum size, the Hardware Inventory Client Agent will move the IDMIF to the \Badmifs folder, and the IDMIF file is not sent to the site server to be processed.

Next is the MIF Collection tab. It has the following options:

Collect IDMIF files Adds a new architecture, and attributes and classes, to the Configuration Manager database.

Collect NOIDMIF files Extends the hardware inventory by adding attributes and classes to existing architectures on a client. They are used to extend, or add, new information about existing Configuration Manager clients to the site database.

Changing the Default MIF Storage Location on a Client

You can change the MIF storage location after the client is installed by modifying the registry keys for the IDMIF and MOIDMIF files.

To change the default location for IDMIF files, follow these steps:

- On the client that you want to change the MIF location settings, select Start ➤ Run, type regedit, and then press Enter to start the Registry Editor.
- 2. Go to the following registry key:
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Client\Configuration\Client
 Properties\IDMIF Directory
- 3. Right-click IDMIF Directory, and click Modify.
- 4. Enter the path to which you want to change.
- 5. Close the Registry Editor.

To change the default storage location for NOIDMIF files, follow these steps:

- On the client that you want to change the MIF location settings, select Start ➤ Run, type regedit, and then press Enter to start the Registry Editor.
- 2. Go to the following registry key:
 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Client\Configuration\Client
 Properties\NOIDMIF Directory
- 3. Right-click NOIDMIF Directory, and click Modify.
- 4. Enter the path to which you want to change.
- **5.** Close the Registry Editor.

Note that this procedure will change the MIF storage location only on the client that you worked on. If you want to make this a site-wide client change, you will have to come up with some kind of script that you will deploy to your Configuration Manager clients.

EXTENDING HARDWARE INVENTORY

Even though Configuration Manager 2007 can automatically inventory hardware information from clients by simply enabling the Hardware Inventory Client Agent, you can also customize hardware inventory to collect information that is not reported by default or add totally new information that you want to be collected that you configure yourself.

You can extend hardware inventory by inventorying additional WMI classes, additional WMI class attributes, registry keys, and other customizations to fit your company's needs. If you need to, you can also modify hardware inventory to reduce the amount of information reported by clients.

Before you go delving into the configuration.mof and sms_def.mof files, you should make sure you have an idea of what you are doing and make backups of all files before you edit them.

A great place to start is the "Start to Finish Guide to MOF Editing" (www.smsexpert.com/MOF/guide.aspx), written by Jeff Gilbert (who is now working for the Microsoft documentation team specifically on Configuration Manager), which is provided by the great folks at SMS Expert. You can also find other information on MOF files at www.smsexpert.com/mof/, including sample MOF edits for SMS 2003.

The MOF guide might need to be revised to work exactly with Configuration Manager, but it will give you a good basis on just what is involved in editing MOF files to get the information you need out of hardware inventory.

You will also find a lot of great resources on MOF editing at MyITforum.com, the best resource on systems management information on the Internet. MyITforum.com has a hoard of information about SMS and Configuration Manager, and the forums and email lists are full of great people who are willing to help you with your questions without making you feel stupid. Swing by and take a look; you won't be disappointed.

Providers Used in Hardware Inventory

When extending hardware inventory that is collected by Configuration Manager clients, the configuration.mof file is modified to inventory client information leveraging a registered inventory data provider. Providers used during client hardware inventory are listed at the top of the configuration.mof file and are registered on clients when they first get a computer policy and then compile the configuration.mof file after the Configuration Manager client is installed. Table 10.3 lists the providers that are used in hardware inventory.

TABLE 10.3:	Default Hardware	Inventory	Providers
IUDEE IO:0:	Delaute Haraware	III V CIII OI Y	LIUVIACIS

PROVIDER	How It Is Used
WMI Data Provider	This provider is used to inventory existing client WMI data class information.
Registry Property Provider	This provider is used to gather information on specific registry keys.
Registry Instance Provider	This provider is used to collect information from multiple registry keys according to specific conditions. The best use for this is to inventory various subkeys under one main registry key that will all have similar data values that you want to inventory without creating more than one reporting class.
View Provider	This provider can be used to join multiple data classes into one class or perform simple WQL queries for inventory reporting.
Asset Intelligence Provider	This provider is used to query specific Asset Intelligence inventory information.

Extending Hardware Inventory Using the configuration.mof File

The configuration.mof file is used to modify data class information inventoried by clients with hardware inventory.

To modify the configuration.mof file, follow these steps:

- 1. Make a backup copy of the configuration.mof file, and put it in a safe location.
- 2. On the primary site server, go to the <Configuration Manager install folder>/ inboxes/clifiles.src/hinv folder.
- 3. Using Notepad, open the configuration.mof file, and make any necessary changes. Figure 10.3 shows part of the configuration.mof file.

FIGURE 10.3 The configuration .mof file



- 4. Close the configuration.mof file, and save the changes.
- 5. Copy the configuration.mof file to the same location that is listed in step 2 to all the primary sites in your hierarchy to propagate the changes to the other sites.

Extending Hardware Inventory Using the sms def.mof File

The sms_def.mof file is used to modify reporting class information inventoried by clients during hardware inventory. The sms_def.mof file contains a list of classes and attributes that relate to data classes stored in the WMI repository of Configuration Manager clients.

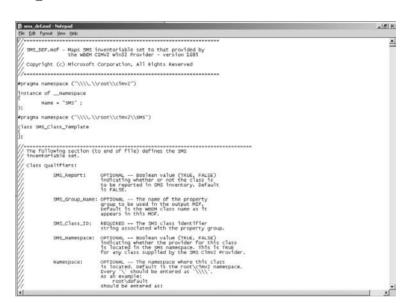
Classes and properties that have the reporting qualifier set to TRUE are collected, and those set to FALSE are not. There is an exception: if a class is set to TRUE, then any class properties that have the key attribute are then collected even if it is set to FALSE.

You can use Notepad to modify the sms_def.mof file just like you can the configuration.mof file. If there are properties or classes that you don't want to use anymore, you can set them to FALSE. If you want to add classes to report, set them to TRUE. Be careful when you do this, because the sms_def.mof file is not made to be used with most or all of its reporting classes set to TRUE. If you go into this file and turn on a lot of things without thinking about it first, you could cause yourself a lot of trouble because an inventory report file that is too big will affect performance on the network. If you decide to edit the sms_def.mof file, first verify the size of a client's complete hardware inventory, and make sure the new size isn't going to cause you problems. After that, test the new sms_def.mof file in your test lab before you replace it on your production Configuration Manager hierarchy.

To modify the sms_def.mof file, follow these steps:

- 1. Make a backup copy of the sms_def.mof file, and put it in a safe location.
- On the primary site server, go to the <Configuration Manager install folder>/ inboxes/clifiles.src/hinv folder.
- **3.** Using Notepad, open the sms_def.mof file, and make any necessary changes. Figure 10.4 shows part of the sms_def.mof file.

FIGURE 10.4
The sms_def.mof file



- **4.** Close the sms_def.mof file, and save the changes.
- Copy the sms_def.mof file to all the primary sites in your hierarchy to propagate the changes to the other sites.

Extending Hardware Inventory Using Third-Party Tools

You can probably see by now that extending hardware inventory is not a task to be taken lightly. Editing classes that are already present in the configuration.mof and sms_def.mof files must be done precisely, or it can cause errors that could corrupt client inventory data. Adding new classes or inventory items takes a lot of intensive research and testing before implementation to make sure that additions work correctly. Even if you rely on the excellent resources of MyITforum.com

to find MOF file additions that other Configuration Manager admins have made, you might not find the exact solution that your organization needs. With that in mind, the company DudeWorks may very well have solved that problem with its Inventory Manager product.

The website, www.dudeworks.com, describes what the software does:

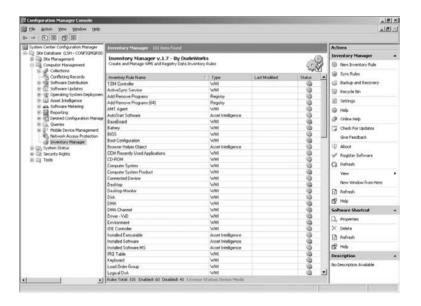
Inventory Manager replaces the manual editing of text-based MOF files with an easy-to-use GUI front end that is integrated with the System Center Configuration Manager 2007 console.

Inventory Manager allows administrators to easily add, edit, and remove inventory rules for hardware and software within Configuration Manager. Using Inventory Manager, administrators can also view and change properties and reporting attributes of built-in inventory rules, as well as create new rules for WMI values and registry keys using simple WMI and registry wizards.

Inventory Manager provides a rule based management solution which takes all the guess-work out of asset inventory and speeds the process of defining and managing inventory items to a few minutes rather than several hours or days.

After installation, Inventory Manager can be accessed from the Configuration Manager console, as shown in Figure 10.5.

FIGURE 10.5 Inventory Manager console add-in



To enable an inventory rule that is already included in the sms_def.mof file, all you have to do is scroll down the list of rules shown in Inventory Manager, double-click the rule you want to enable, and go to that rule's reporting properties, as shown in Figure 10.6 and Figure 10.7.

Inventory Manager also makes backups of your MOF files automatically when you make changes, and it allows you to restore backups if you discover a problem later, as shown in Figure 10.8.

You can also sync your MOF changes to your child sites right from the console, as shown in Figure 10.9.

For more information about Inventory Manager and all of its features, check out www.dudeworks.com.

FIGURE 10.6 Inventory Rule Reporting Properties dialog box's General tab

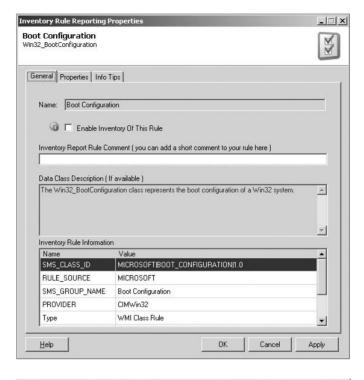


FIGURE 10.7 Inventory Rule Reporting Properties dialog box's Properties tab

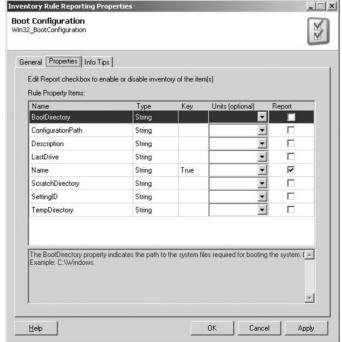
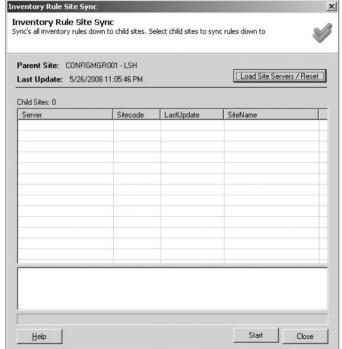


FIGURE 10.8
Inventory Manager
backup and recovery



FIGURE 10.9
Inventory rule site sync

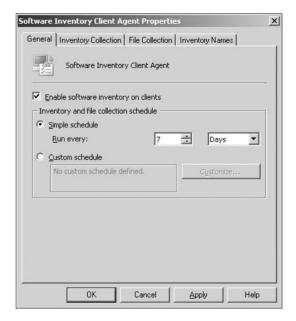


Configuring Software Inventory for a Configuration Manager Site

To configure software inventory for a site, you must, as with hardware inventory configuration, have the Modify permission for the site. Then follow these steps:

- **1.** In the Configuration Manager console, select System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ site code ➤ site name ➤ Site Settings ➤ Client Agents.
- 2. In the left pane, right-click Software Inventory Client Agent, and then click Properties.
- **3.** The first thing you will see is the General tab, shown in Figure 10.10.

FIGURE 10.10
General tab of the
Software Inventory
Client Agent



- 4. From here you can enable software inventory and set a schedule just like you did with hardware inventory.
- **5.** Next is the Inventory Collection tab, shown in Figure 10.11. The first section on this tab is File Types, where you can add or delete types of files that you want to use. Clicking the New button opens a dialog like that shown in Figure 10.12.
- **6.** Type the file or file type in the first box. As it says in the dialog box, you can use wildcards for the filename. You can use ? for any one character that you don't know, and you can use * for everything else (for example, *.exe would find all the .exe files).
- 7. Clicking the Set button opens the dialog box shown in Figure 10.13. Here you can specify to search all the hard disk drives on the client (not the networked drives), a specific patch if you want to narrow your search, or a path variable if that might change from computer to computer (like the Windows directory).
- **8.** The next section on the Inventory Collection tab is Reporting Detail. The File Details option will display all scanned files, including unknown files (files without manufacturer data) in Resource Explorer under the File Details section. This is selected by default.

FIGURE 10.11 Inventory Collection tab of the Software Inventory Client Agent

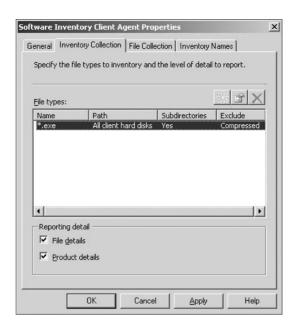


FIGURE 10.12 Inventoried file properties

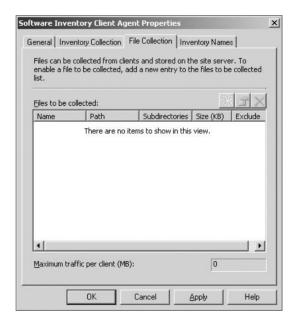


- **9.** The Product Details option will list files in Resource Explorer only when manufacturer details are present. This is selected by default.
- **10.** The File Collection tab is next (Figure 10.14). This is very dangerous territory, so think hard about what you are doing before selecting this option; it could cause a large amount of network traffic.
- 11. The Files To Be Collected section is where you actually add the files that you want collected, and the dialog box for adding a new file is similar to the one for adding files to Inventory Collection; the only difference is the Maximum Size (KB) option for the file that you want to collect. Figure 10.15 shows the Collected File Properties dialog box.

FIGURE 10.13
File Path Properties dialog box



FIGURE 10.14
File Collection tab



- **12.** Next is the Inventory Names tab (Figure 10.16). As discussed earlier in the chapter, software manufacturer names are not always standardized in the file header information. You can use this tab to change variations of manufacturer names into a consistent one.
- **13.** Two name types can be configured, Manufacturer and Product, for each display name and inventoried name set. Configure each section to show software names to your liking
- 14. In the Inventoried Names section, you can use these wildcard variables:

%	Any string of zero or more characters
_ (underscore)	Any single character
[] (brackets)	Any single character within a range
[^]	Any single character <i>not</i> with a range

FIGURE 10.15 Collected File Properties dialog box

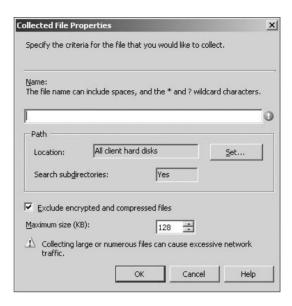
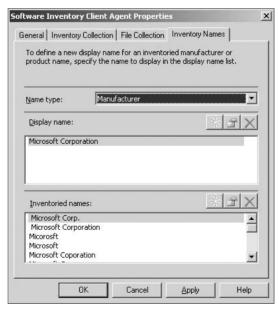


FIGURE 10.16
Inventory Names tab



When you are done configuring the options that you want, click OK to save your changes.

MISCELLANEOUS INVENTORY CONFIGURATIONS AND OPTIONS

The following sections cover some configuration options for inventory that don't neatly fit into other categories.

ENCRYPTING CLIENT INVENTORY REPORTS

In Mixed mode, a site will automatically sign but not encrypt inventory reports for clients. For better security for inventory on a Configuration Manager site, it is recommended you enable inventory encryption when in Mixed mode for the best security.

To enable inventory encryption, follow these steps:

- **1.** In the Configuration Manager console, select System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ site code ➤ site name.
- **2.** Right-click *site code* ➤ *site name*, and click Properties.
- 3. Click the Site Mode tab.
- In the Client settings section, select the Encrypt Data Before Sending To Management Point check box.
- 5. Click OK to finish.

EXCLUDING FILES FROM SOFTWARE INVENTORY

This a "secret" left over from at least SMS 2.0 that allows you to place a special file named skpswi.dat on the root of a drive, or just in one or more folders, to exclude it from software inventory. (This doesn't work with mobile device client inventory, though.) Once this file is placed, software inventory will not inventory the drive or folder again, until that file is removed.

To exclude files from software inventory, follow these steps:

- 1. Using Notepad, make an empty file named skpswi.dat.
- Right-click that file, and click Properties. In the file properties for skpswi.dat, select the Hidden attribute.
- **3.** Place the skpswi.dat file at the root of the drive or folder that you don't want to collect software inventory.

VIEWING COLLECTED FILES

Before trying this procedure, make sure you have the Read and View Collected Files permissions for the site.

To view the collected files of a particular client, follow these steps:

- In the Configuration Manager console, select System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Collections.
- 2. Open Collections so you can see more details, and find the collection that will have a client that you know will have collected files.
- Once you have found the client you want, right-click it.
- **4.** Then click All Tasks and then Start Resource Explorer.
- **5.** In the left pane, select Software.
- **6.** Then click Collected Files. You will see a list of all the files that have been collected from that client in the right pane.

- 7. To view a file, you have two options:
 - ◆ Right-click a file, select All Tasks, and click View Files to look at the file.
 - Right-click a file, select All Tasks, and click Save to save the file to another location so you can view it in an application of your choice.

Troubleshooting Inventory

The following sections cover some basic information that will help you troubleshoot specific problems.

CLIENTS WITH LOW RESOURCES MIGHT NOT RUN SOFTWARE INVENTORY

The first thing that software inventory does when its starts an inventory cycle on a client is check to make sure that there are enough resources available to continue. A client must have at least the following resources for an inventory cycle to start:

- ◆ The client must have 3MB of virtual memory.
- ◆ The client must have 500KB of free disk space.
- ◆ If you are using file collection, clients must have enough free drive space for 210 percent of all the files that are to be collected, since the Software Inventory Client Agent will make copies of all the files that it is going to collect before it sends them to its management point.

If the client doesn't have enough resources when an inventory is scheduled to run, it will try again within 24 hours.

WHEN CLIENTS TRY TO INVENTORY DATA CLASSES THAT DON'T EXIST

As we have already discussed, the Hardware Inventory Client Agent gets information about a computer's hardware from the WMI data classes. Sometimes not all of the WMI data classes that Configuration Manager is set up to inventory are present on a client.

Clients with different operating systems are a good example of this. The sms_def.mof file is configured to inventory certain new WMI classes in Windows Vista that aren't available on other operating systems. The Hardware Inventory Client Agent will still try to inventory those classes on a Windows XP or Windows 2000 client since they are included in the sms_def.mof file.

When a client tries to inventory a class that doesn't exist, you will see an entry only in the InventoryAgent.log file, because no status message will be sent to the site server. If you need to figure out whether a client is trying to inventory nonexistent data classes, you will see entries similar to Collection: Class "<Class Name>" does not exist in InventoryAgent.log.

PROBLEMS WITH DATA STRINGS THAT ARE LONGER THAN 256 CHARACTERS

If the Hardware Inventory Client Agent finds a property of a data class that has a string value with more than 256 characters, then the management point will not process that property, and its information will not be stored in the Configuration Manager database.

When this happens, you will see entries in the MP_Hinv.log file similar to the following:

Hinv: warning skipping instance of array property as exceeds max length. Class: "<data class name>" Property: "<data class property>"

CUSTOM ERROR CODE FOR INVENTORY

WMI corruption has been a common problem with Configuration Manager clients, since previous versions of the product. To help identify this problem when it happens, Microsoft has included a custom error code for inventory.

Table 10.4 lists the custom error code for inventory.

TABLE 10.4:	Custom	Error Code for I	nventory
IADLE IV.4.	Custom	citoi Code ioi i	nventorv

ERROR CODE	POSSIBLE PROBLEM	Possible Solution
0x80040900	A valid WMI instance	Rebuild the WMI database.

Software Metering in Configuration Manager 2007

The Software Metering feature in predecessors of Configuration Manager 2007 had a somewhat checkered past among veteran SMS administrators.

When SMS 2.0 was released, Software Metering was a nightmare to configure and implement and was barely usable in a consistent manner. That version of Software Metering was designed by a third-party vendor and was not really up to the task it was designed for, and the community of SMS administrators let Microsoft know about it. Software Metering might have been one of the first features that started the intense community involvement between Microsoft and its customers, which you can still see in the MyITfourm.com community even today.

As the years of SMS 2.0's product life went on, Microsoft received more and more feedback on its features from its users and how SMS needed to be improved to make it a better product. By the time that SMS 2003 came around, Microsoft had redesigned Software Metering itself from the ground up and made it a useful feature as originally promised.

In Configuration Manager 2007, Microsoft has continued this trend, because Software Metering is better than ever.

What's New in Software Metering for Configuration Manager 2007

In Configuration Manager 2007, Microsoft has added a new feature to Software Metering, called *Automatic Rule Generation*, which will help administrators a great deal in figuring out exactly which applications should be monitored in their environments.

Automatic rule generation allows you to set up software metering to configure software metering rules automatically from recent usage inventory data that is in the Configuration Manager database. You can configure automatic rule generation so that only applications used on a certain percentage of computers that you specify will have metering rules created. You can also set the maximum number of automatically generated rules on a per-site basis.

You'll learn more about this new feature later in the chapter.

Overview of Software Metering

Software Metering in Configuration Manager 2007 allows you to monitor and collect information about software usage on Configuration Manager clients. The information collected is based on the software metering rules that can be configured in the Configuration Manager console or created automatically based on usage data collected by inventory.

The Software Metering Client Agent on each client evaluates these rules, collects the requested data, and then reports it to the Configuration Manager database. The Software Metering Client Agent will continue to collect usage data even if can't connect to its management point and will send the collected data on to the site server after it regains a connection.

Software metering data is held on the site server until it is summarized every so often on a set schedule, and then it is forwarded up the Configuration Manager hierarchy to a parent site. If more than one parent site reports to a central site, each parent will summarize the data from all of their sites and then forward that data up to the central site server. When the process is done, all the software metering data from all clients in the hierarchy will be in the central site database.

By default, software metering rules are active only on the Configuration Manager site that they are created on. To make sure that your software metering rules are consistent throughout your hierarchy, create all of your software metering rules at the top site of your hierarchy, and choose the option that each rule should be copied to all child sites.

After you have waited a while for software metering data to be collected from clients, you can use other Configuration Manager features, such as reporting, queries, and collections, to view that collected data. Combined with software inventory, this gives administrators a powerful tool to help answer questions that come up in every IT organization. Examples of these questions include the following:

- What is the relationship between how many instances of a software program are installed on clients in relation to how many actually use that software?
- Do you need to buy more licenses when renewing your license agreement with a software vendor?
- ♦ What users are still using an obsolete program before you plan an upgrade?
- Is anyone playing Solitaire on company computers?

Configuring Software Metering

To use software metering, you must enable the Software Metering Client Agent, which is not enabled by default. When you enable software metering, the setting will be downloaded to clients according to the policy polling interval that is set in Computer Client Agent Properties in the Configuration Manager console. That setting is every 60 minutes by default.

ENABLING THE SOFTWARE METERING CLIENT AGENT

Take these steps to enable the Software Metering Client Agent:

- In the Configuration Manager console, select System Center Configuration Manager ➤ Site
 Database ➤ Site Management ➤ site code ➤ site name ➤ Site Settings ➤ Client Agents.
- 2. Right-click Software Metering Client Agent, and then click Properties.
- **3.** On the General tab, select Enable Software Metering On Clients.
- **4.** Click OK to finish.

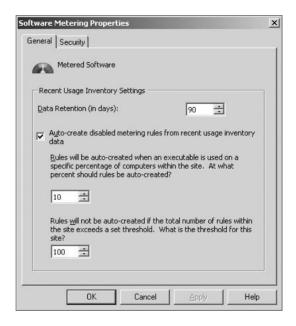
CONFIGURING AUTOMATIC SOFTWARE METERING RULE GENERATION

As discussed earlier in the chapter, Configuration Manager introduces a new feature that allows software metering to generate rules automatically from recent usage inventory based on criteria that you specify, leaving the rules disabled until you enable them. You can configure these rules

so that only applications that are used on a certain percentage of clients will have rules created. You can also set what the maximum number of automatic rules will be generated for the site. To configure automatic rule generation, follow these steps:

- In the Configuration Manager console, select System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Metering.
- 2. Right-click the Software Metering node, and then click Properties.
- **3.** This opens the General tab the Software Metering Properties dialog box, as shown in Figure 10.17.

FIGURE 10.17
General tab of the Software Metering Properties dialog box



You can set the following options:

- Specify the amount of time in Data Detention (In Days) that data generated by software rules will be held in the site database. The default setting is 90 days.
- Select the Auto-create Disabled Metering Rules From Usage Inventory Data box.
- Set the percentage of computers in a Configuration Manager site that must use an executable before a software metering rule for that executable is automatically created. The default setting is 10 percent.
- Set the maximum number of rules that software metering will automatically generate. The default setting is 100 rules.
- 4. When you are done setting your options, click OK.

ENABLING AND DISABLING SOFTWARE METERING RULES

You don't have to delete a rule if you don't want to use it; instead, you can enable it or disable it as you need to if you want to keep it.

To enable or disable a software metering rule, follow these steps. Figure 10.18 shows automatically generated software metering rules in the Configuration Manager console.

FIGURE 10.18
Software Metering node with software metering rules



- In the Configuration Manager console, select System Center Configuration Manager ➤ Site
 Database ➤ Computer Management ➤ Software Metering.
- **2.** Right-click one or more rules that you want to configure, and then click either Enable or Disable. The option that is available will depend on what state the rule is already in.

ADDING A SOFTWARE METERING RULE

If the automatically generated rules aren't what you need, then you can manually make your own to meet your organization's needs. To make your own software metering rules, follow these steps:

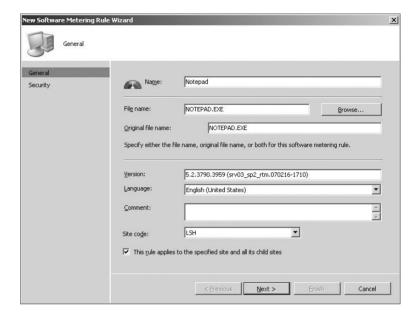
- In the Configuration Manager console, select System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Metering.
- 2. Right-click the Software Metering node, click New, and then click Software Metering Rule.
- This opens the General page of the New Software Metering Rule Wizard, shown in Figure 10.19.

This page has the following options:

- Name: The name of the software metering rule, which should be unique. You can have rules with the same name, as long as the filenames are different.
- File Name: The name of the executable file you want to meter. You can click Browse to display the Open dialog box where you can select the file that you want to meter. You can manually type in this filename, but when you do that, no checks are made to determine whether the file exists or whether it contains the needed file header information. For the best results, always use the Browse button if possible. Wildcard

characters can't be used in this field, and selecting the Original File Name field is optional.

FIGURE 10.19
General page of the
New Software Metering Rule Wizard



- ◆ Original File Name: The name of the executable file that you want to meter. This name is matched to the information in the file header, not the filename itself, so you still meter it if the file is renamed. Wildcard characters can't be used in this field, and selecting the File Name field is optional.
- ◆ Version: The version of the executable file that you want to meter. If you use the Browse button to select your file, this field will be filled out automatically from the file's header information (as shown in Figure 10.19). You can use the wildcard character (*) to represent any string of characters or the wildcard character (?) to represent any single character. If you want to meter all versions of the file, you can use the default value (*).
- ◆ Language: The language of the file that you want to meter. The default value is English (United States). If you use the Browse button to select your file, then this is filled out automatically from the file's header information. If you want to meter all language versions of this file, then select Any from the drop-down list.
- ◆ Comment: A description that you want for the rule. This is an optional field.
- Site Code: The Configuration Manager site code that the software metering rule will apply to.
- ◆ This Rule Applies To The Specified Site And All Its Child Sites: This is pretty self-explanatory. If you want this rule to be passed down the Configuration Manager hierarchy, select this box.
- 4. Once you have filled in all the information, click Next.

5. That opens the Security page of the wizard, which allows you to specify any optional class and instance rights for this rule. Once you are done, click Finish.

DELETING SOFTWARE METERING RULES

When you delete a software metering rule, the change will be downloaded to clients during their next policy polling interval, just like when you create rules.

To delete a software metering rule, follow these steps:

- In the Configuration Manager console, select System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Metering.
- 2. Find the metering rule that you want to delete, right-click it, and then click Delete.
- **3.** You will then see a Confirm Object Delete dialog box. If you are sure that you want to delete this rule, then click Yes.

SOFTWARE METERING MAINTENANCE TASKS

Depending on how you configure software metering, you could end up with a lot of data collected in the Configuration Manager database. To help you manage that data, several maintenance tasks are included in the Configuration Manager console.

There are four tasks in total in two categories — two tasks for deleting aged software metering data and two tasks for summarizing software metering data.

All of these tasks are enabled by default. To find them in the Configuration Manager console, select System Center Configuration Manager > Site Database > Site Management > site code > site name > Site Settings > Site Maintenance > Tasks. Then double-click the task you want to configure.

These tasks summarize software metering usage data to compress the amount that is stored in the Configuration Manager database. For the data summarization tasks to succeed, there has to be software metering data that is at least 12 hours old.

Summarization runs daily by default and will run only against data that is at least 12 hours old. This is required for all software metering reports to produce any meaningful data. To get an idea of what is in the most current set of summarized data, you have to know when that last summarization took place. The report Software Metering Summarization Progress has been included as a stock report in Configuration Manager to give that information.

The Summarize Software Metering File Usage Data task concentrates software metering file usage data from several records into one. This record gives information about the program name, version, language, and number of distinct users over intervals of 15 minutes to 1 hour. This process compresses and optimizes the amount of data stored in the Configuration Manager database.

For every hour and every 15-minute time frame within the hour, this task will calculate the total number of distinct user/computer combinations that are running the programs that are being metered. Within 15-minute intervals, this will give an approximate number of concurrent users of a metered program.

When software summary data is sent up the Configuration Manager hierarchy, the data from each site is kept separated from the data from the other sites. When the data reaches a parent site, each record is marked with the site code of the site it came from.

The Summarize Software Metering Monthly Usage Data task concentrates detailed software metering usage data from many records into one. This record gives information on the program name, program version, language, program running times, number of times used, last time used, username, and computer name. This summarization compresses the amount of data that is stored in the Configuration Manager database and is sent to the central site.

The summary data also includes the number of times each matching metered software ran on a specific computer by a specific user during that month. This task is set to run every day by default, and the summary is done for a period of one month.



HOW MANY DO WE HAVE TO UPGRADE?

You hear that Adobe Reader has a patch for a vulnerability in the software, and you need to get a rough estimate of how many instances are on computers that you need to upgrade for an upcoming meeting.

You know that the main Acrobat Reader executable is called AcroRd32.exe and that all versions 8.1.037 are affected. To get that information, you go to the Count Computers with a Specific File Name report, which is based on software inventory information and input AcroRd32.exe in the Report field. After clicking Display, you get the total numbers of AcroRd32.exe sorted by version number.

The Bottom Line

Configure and manage Software Inventory Even though Software Inventory hasn't changed much in Configuration Manager 2007, it is still a very effective tool in the battle of keeping track of what software is on your network.

Master It Eventually you might need to add to the files and file types that are part of the inventory collection in the software inventory of your hierarchy. Where would you go to do that?

How to configure and manage Hardware Inventory Hardware Inventory provides a wealth of information on the hardware resources in your organization. That information is vital when planning for things such as updating standard business software or upgrading the standard operating system your organization uses. If the standard hardware inventory collected is not enough for your needs, then you have many options to extend hardware inventory to get that vital information.

Master It What part of Hardware Inventory is contained in the sms_def.mof file?

How to configure and manage Software Metering Keeping track of software that is installed and actually being used is a large part of being able to manage software licenses effectively. With Software Metering in Configuration Manager paired with Software Inventory, you can get detailed information on just what software is out there and who is or is not using it. This goes a long way to help keep your software licensing in compliance.

Master It How long do you have to wait, at the very least, after you configure Software Metering before you can expect to see any data returned?

Chapter 11

Reporting

Now that Chapter 10 has discussed software inventory and metering in Configuration Manager, we can move on to look at its Reporting component.

In Configuration Manager 2007, the Reporting feature is much like the version found in Systems Management Server 2003. Microsoft has added some new reports, but the basic functionality is the same.

Reporting is probably the feature of Configuration Manager 2007 most widely used outside of Information Technology departments. In other words, it can be set up to allow other departments to view data within the Configuration Manager hierarchy. Not every organization will allow the data within Configuration Manager to be viewed outside the department, but this information can be extremely valuable to many departments within an organization.

With that in mind, in this chapter you learn skills that will help you create reports that are accessible only to the individuals or groups you intend, customize reports to fit your organization, create your own reports, and share these reports with other Configuration Manager administrators.

In this chapter, you learn to

- Set up Reporting Point roles
- Create and manage reports
- Create and manage security on a single report
- Create and manage dashboards

Setting Up Reporting Point Roles

As discussed in Chapter 4, activating various roles for a server is as simple as checking a check box. However, as with anything that appears simple, there is more than meets the eye. Here is a more detailed list of the steps required for setting up a Reporting Point role.

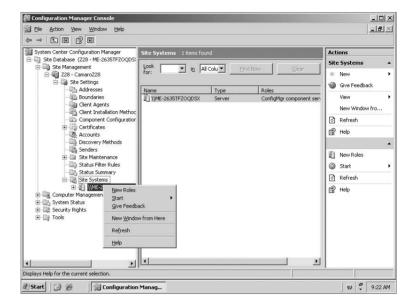
Installation of the Reporting Point Role

The installation of the Reporting Point role is fairly straightforward, but of all the features within Configuration Manager 2007, this could be the one most used by people outside the Information Technology group. If allowed within your organization, this role can be given out to other departments or managers so they can view reports. The reports can be locked down based on security models built within Configuration Manager, as we will discuss later in this chapter.

To configure a Reporting Point, take the following steps:

- 1. Expand the Site Management node.
- **2.** Expand the Site node, followed by Site Settings and then Site Systems.
- **3.** Right-click on the name of your primary site server and select New Roles, as shown in Figure 11.1.

FIGURE 11.1
You begin enabling a
Reporting Site role by
selecting New Roles for
the primary site server.



- **4.** This launches the New Site Role Wizard. On the opening screen, select Next to display the General page, shown in Figure 11.2.
- Under Available Roles, select the Reporting Point check box, as shown in Figure 11.3, and then select Next.
- **6.** Specify the folder for your Configuration Manager Reporting. This folder will be the virtual directory that will be used within IIS. Make a note of the URL; it will be used to access the Web Reporting tool from a browser. When you are finished, select Next.
- 7. Review the Summary Details and select Next, shown in Figure 11.4.
- **8.** Select Close.
- Review the rsetup.log on the Primary Site Server logs directory to make sure it shows Return 0 and Finished.
- 10. Review the SMSReportingInstall.log to make sure it shows Installation of Reporting Point Complete.

FIGURE 11.2
The General page of the
New Site Role Wizard

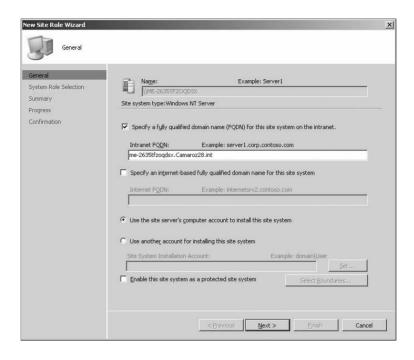


FIGURE 11.3
The System Role Selection page of the New
Site Role Wizard

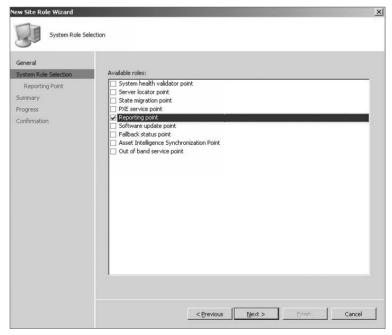
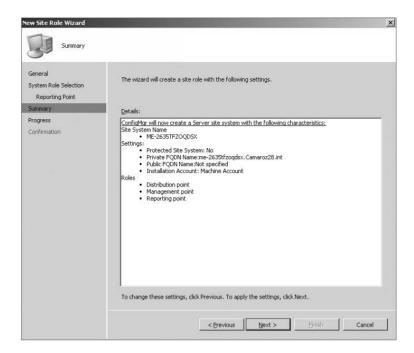


FIGURE 11.4
Summary Details



Viewing the New Virtual Web Directory in IIS

Adding the Configuration Manager Reporting role creates a new Virtual Web Directory under Internet Information Services (IIS). To view the settings under IIS, follow these steps.

- Open up the Administrative Tools folder and click the Internet Information Services (IIS) Manager icon.
- **2.** Expand the Web Sites Container, and then expand Default Web Site.
- **3.** Verify that the Virtual Directory folder created in the installation procedure is displayed, as in Figure 11.5.

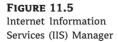
Default Reports

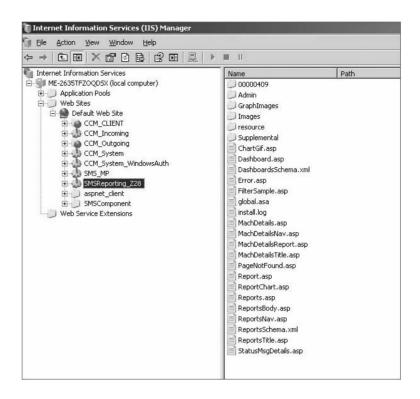
By default, the Reporting Role adds 369 reports, including the 130 Asset Intelligence reports discussed in Chapter 9. By default, the reports consist of the following categories,

Asset Intelligence Allows administrators (and anyone else granted permission) to report inventory and manage software license usage throughout the Configuration Manager enterprise by using the Asset Intelligence Catalog.

Desired Configuration Management — **Assignment** Allows administrators and others to report on Desired Configuration Management Assignment for a computer or collection.

Desired Configuration Management — Compliance Allows administrators and others to report on Desired Configuration Management Compliance for a computer or collection.



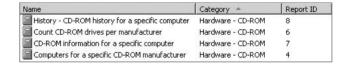


Desired Configuration Management — **Errors** Allows administrators and others to report on Desired Configuration Management Errors with the enterprise.

Device Management Allows administrators and others to report on Device Management.

Hardware — **CD-ROM** Allows administrators and others to report on various CD-ROMs; available reports are shown in Figure 11.6.

FIGURE 11.6 Hardware – CD-ROM reports



Hardware — **Disk** Allows administrators to report on various disk configurations.

Hardware — **General** Allows administrators and others to report on general hardware of clients.

Hardware — **Memory** Allows administrators and others to report on memory configurations of clients.

Hardware — **Modem** Allows administrators and others to report on modem configurations.

Hardware — **Network Adapter** Allows administrators and others to report on Network Adapter configurations of a client; available reports are shown in Figure 11.7.

FIGURE 11.7 Hardware – Network Adapter reports

Name	Category -	Report ID
Computers with a specific network adapter	Hardware - Network	29
Count network adapters by type	Hardware - Network	31
Network adapter information for a specific com	Hardware - Network	30

Hardware — **Processor** Allows administrators and others to report on various processor configurations of a client.

Hardware — **SCSI** Allows administrators and others to report on various SCSI cards and configurations of a client.

Hardware — **Sound Card** Allows administrators and others to report on Sound cards within a client.

Hardware — **Video Card** Allows administrators and others to report on various configurations of video cards of clients.

Network Allows administrators and others to report on various Network settings.

Network Access Protection Allows administrators and others to report on Network Access Protection configurations.

Operating System Allows administrators and others to report on various OS-related items and configurations.

SMS Site — **Client Information** Allows administrators and others to report on client information as it pertains to the SMS site.

SMS Site — **Discovery and Inventory Information** Allows administrators and others to report on Discovery and Inventory information such as when the last discovery information was collected.

SMS Site — General Allows administrators and others to report on various site settings.

SMS Site — **Server Information** Allows administrators and others to report on various site servers.

Software — **Companies and Products** Allows administrators and others to report on various software installed within the enterprise.

Software — **Files** Allows administrators and others to report on collected or inventoried files.

Software Distribution — **Advertisement Status** Allows administrators and others to report on status of advertisements.

Software Distribution — Advertisements Allows administrators and others to report on advertisements.

Software Distribution — **Collections** Allows administrators and others to report on collections and when they were last updated.

Software Distribution — **Packages** Allows administrators and others to report on packages.

Software Metering Allows administrators and others to report on various software metering and when the application was last opened. Available reports are shown in Figure 11.8.

FIGURE 11.8 Software Metering reports

Name	Category A	Report ID	
All software metering rules at this site	Software Metering	109	
Computers that have a metered program install	Software Metering	120	
Computers that have run a specific metered so	Software Metering	116	
Concurrent usage for all metered software pro	Software Metering	117	
Concurrent usage trend analysis of a specific m	Software Metering	110	
Install base for all metered software programs	Software Metering	113	
Software metering summarization progress	Software Metering	142	
Time of day usage summary for a specific mete	Software Metering	114	
Total usage for all metered software programs	Software Metering	118	
Total usage for all metered software programs	Software Metering	119	
Total usage trend analysis for a specific metere	Software Metering	111	
Total usage trend analysis for a specific metere	Software Metering	112	
Users that have run a specific metered softwar	Software Metering	115	

Software Updates — **A. Compliance** Allows administrators and others to report on Software updates.

Software Updates — **B. Deployment Management** Allows administrators and others to report deployments of software updates.

Software Updates — **C. Deployment States** Allows administrators and others to report on various states of deployment of software updates.

Software Updates — **D. Scan** Allows administrators and others to report on scans for software updates.

Software Updates — **E. Troubleshooting** Allows administrators and others to report on issues with software updates.

Software Updates — **F. Distribution Status for SMS 2003 Clients** Allows administrators and others to report on software updates for SMS 2003 clients.

State Migration Allows administrators and others to report on migration states.

Status Messages Allows administrators and others to report on status messages.

Status Messages — **Audit** Allows administrators and others to report on status messages.

Task Sequence — Advertisement Status Allows administrators and others to report on Task Sequences Advertisement status.

Task Sequence — **Advertisement** Allows administrators and others to report on advertisements within Task Sequence.

Task Sequence — **Progress** Allows administrators and others to report progress of task sequences.

Task Sequence — References Allows administrators and others to report references of task sequences.

Upgrade Assessment — Windows Vista Allows administrators and others to report if clients are able to be upgraded to Windows Vista.

Upgrade Assessment — Windows XP Allows administrators and others to report if clients are able to be upgraded to Windows XP.

Users Allows administrators and others to report on users within the environment.

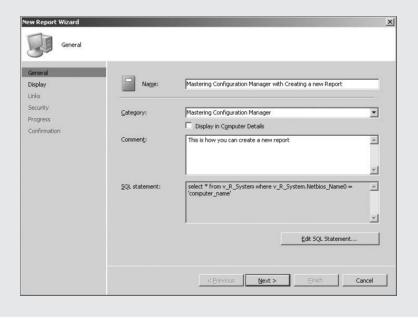
Wake on LAN Allows administrators and others to report on Wake on LAN progress.

As you can see, Microsoft has done a good job of providing some key reports that are ready to use out of the box. The categories are completely customizable, so if you want to change the categories to match your own desires, you can. You can create your own custom categories as well.

CREATING A CUSTOM REPORT

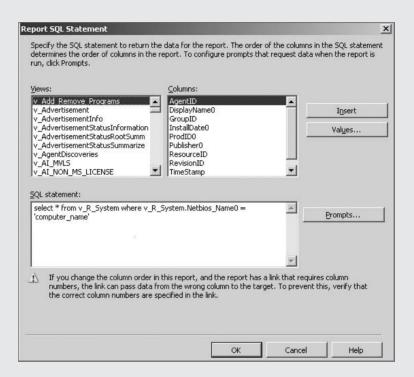
Many times you will be faced with having to create your own custom report in order to generate a report that will properly show the information needed. To create your own report, follow these steps:

 Right click on the Reports node, select New, and then choose Report. This will open the New Report Wizard, as shown here:



Fill in the information, being as descriptive as possible so you or anyone else seeing the report name will fully understand what the report will display once the report is viewed.

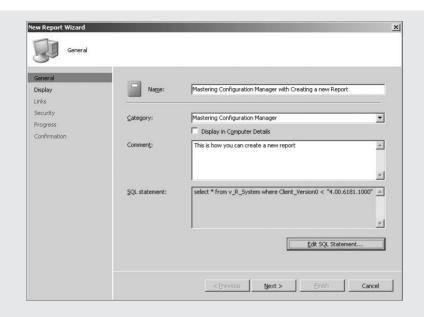
Click the Edit SQL Statement button to define the SQL statement you will use within your report:



3. Type in the SQL statement for your report and then choose OK. In this example, we will be using the following SQL statement to find clients that do not have the latest Configuration Manager client version:

```
select * from v_R_System where Client_Version0 < "4.00.6181.1000"</pre>
```

Now you will be back at the New Report Wizard with all the information properly filled in, as shown here.



4. Click Next and then select the refresh rate. For this example, we will use the default values, so you can choose Next. Because this report will not be linking either, select Next in the next dialog box as well. Then choose Finish.

Now you can run the report you just created in order to show all the clients with a client version less than 4.00.6181.1000.

Viewing Available Reports

You can view the list of available reports from within the Configuration Manager administrator console or through the Web Reporting node created during the configuration of the Reporting role. Figure 11.9 shows the Reporting node expanded from within the Configuration Manager administrator console, and Figure 11.10 shows the Report Viewer running in a web browser.

As you can see, the Report Viewer is grouped by the categories within Configuration Manager. The Configuration Manager administrator console lists the reports alphabetically.

The default reports will not always show the information you want or need for your infrastructure. Sometimes you might have to take one of these reports and customize it to meet your needs, or you might have to create an entirely new report in order to display the information you need for your reports. Microsoft understood this need and built in a way to create and manage reports.

FIGURE 11.9
Viewing available
reports in the Reports
node

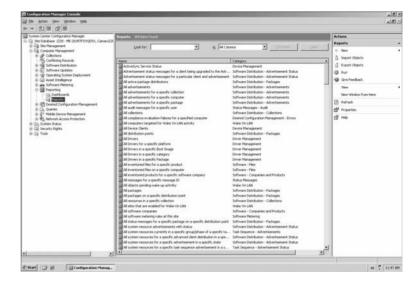


FIGURE 11.10
Viewing available
reports in the Report
Viewer



Running a Report

There are two ways to run a report. The first is to use the Configuration Manager administrator console and the second is to use the web-based Report Viewer. Depending on your preferences, you might choose to use the Configuration Manager console to run your reports. However, our

preference is to run the reports from the admin console only if we are already in the console, and to use the web-based version otherwise, because it seems to be faster.

Note that you cannot create new reports within the web-based version; you must use the administrator console in order to create new reports.

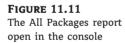
Running a Report from the Administrator Console

To run a report using the Configuration Manager administrator console, follow these simple steps:

- Open the Configuration Manager administrator console and expand Site Database.
- 2. Expand the Computer Management node, followed by the Expand Reporting node and then Expand Reports.
- **3.** Browse to the report you want to run, right-click, and choose Run.

This will open the report within the Configuration Manager administrator console. You can choose to Copy, Export, Print, Add to Favorites, and/or E-Mail the report. A sample report is shown in Figure 11.11, demonstrating some but not all of the available options once you have the report open:

- If you choose Copy, the contents of the report data and column headings are copied to the clipboard, so you can paste the information in whatever form you desire.
- If you choose Export, the contents of the report data and column headings are copied to a CSV file, which you can then open with Excel or another program.
- ◆ If you choose Print, the report will be printed out to the printer you chose.
- If you choose Add to Favorites, the report URL will be saved in your browser Favorites so you can view the report at a later date.
- If you choose E-Mail, the URL will be e-mailed to whomever you address the e-mail.





Running a Report from the Report Viewer

To run a report using the web-based Report Viewer, follow these simple steps:

- 1. Open your web browser to the URL for the Report Viewer. As described earlier in the chapter, this URL is the location you specified when setting up the Reporting Point role.
- **2.** Expand the category of the report you want to run.
- 3. Click on the report you want to run.
- **4.** In the Report Information menu on the right, click the Display icon, shown in Figure 11.12. A new window of the report will now be displayed.

FIGURE 11.12 Click the Display icon in the Report Information area to display the report contents.



Choosing a Technique

Both techniques for opening a report result in exactly the same web-based report. We prefer to use the Report Viewer tool because it allows you to grant other users the ability to view reports without having to install the Configuration Manager console on everyone's machine. You can set permissions on individual reports to ensure that end users are only able to see the reports you give them access to view.

Creating and Managing Reports

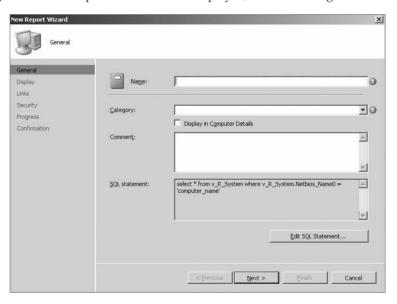
The simplest way to begin creating a new report is to start with a report that includes most of the information you are looking for and then build off that until you get comfortable with building your own reports. There is no need to reinvent the wheel when it comes to reports. As we will discuss later in this chapter, you can even export your custom reports to share with others. You can even take someone else's custom report and import it into your Configuration Manager infrastructure.

Creating a New Report from the Console

You access the data from Configuration Manager stored in the site server through SQL *views*. SQL views are essentially virtual tables that do not themselves contain any data, but are based on tables that contain data. The data is dynamically compiled from source tables when the view is referenced. To create a report, you must either use SQL scripting techniques, import a MOF file, or create a report using the administrator console; you cannot create a report within the Report Viewer tool. Later in the chapter, we will look at the importing and SQL scripting methods The following steps demonstrate the process for creating a new report from the console, using the New Report Wizard.

- Open the Configuration Manager administrator console and expand Site Database.
- **2.** Expand the Computer Management node and then the Reporting node.
- 3. Right-click on the Reports node and choose New Report.
- 4. The General page of the New Report Wizard will be displayed, as shown in Figure 11.13.

FIGURE 11.13
The General page of the New Report Wizard



- **5.** Fill out the data. The comment section is optional. You can either choose a category from the drop-down list or create a new one.
- Click the Edit SQL Statement button to bring up the Report SQL Statement window, shown in Figure 11.14.
- 7. Edit the SQL statement to gather the desired information into a report. In this example, we are using the following SQL statement:

```
SELECT count(model0) as Count, Model0, Manufacture0 from v_gs_Computer_system GROUP BY Model0, Manufacturer0 ORDER BY count DESC
```

Figure 11.15 shows the completed query in the Report SQL Statement window.

FIGURE 11.14
Defining the report in the Report SQL Statement window

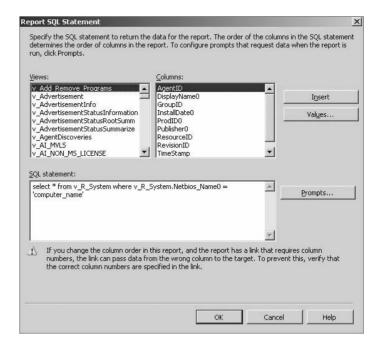
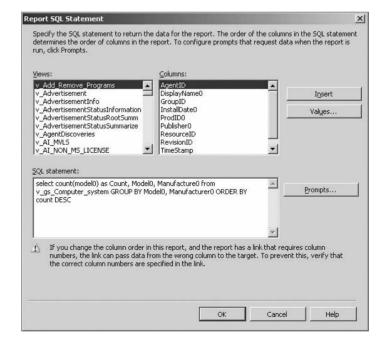
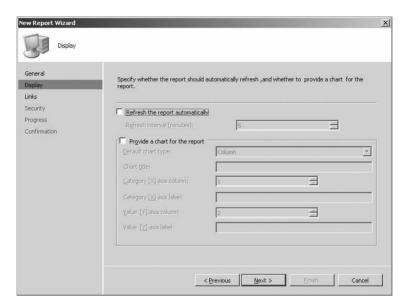


FIGURE 11.15
The completed SQL statement



- 8. Click OK, and now you are back at the New Report Wizard. Click Next.
- **9.** In the Display dialog box of the wizard, shown in Figure 11.16, you have the options to specify whether the report should automatically refresh, and whether to provide a chart for the report.

FIGURE 11.16
Display dialog box



10. In the next page of the wizard, specify whether this report should be linked to another report or other target.

Your options are to link to another report, to Computer Details, to Status Message Details, or to a URL. The next dialog box varies depending on your choice here. In this example, we are choosing No link.

- Now you are prompted for the Security Dialog box. Specify your security setting for this report and click Next.
- **12.** You are presented with the Wizard Completed dialog box. Click Close and you are ready to start using your newly created report.

You can use prompts within your report to make richer reports with greater flexibility. Prompts will allow you to narrow the scope of the data that you will be reporting on. You can have multiple prompts within each report to make the reports as granular as possible.

ADDING LINKS TO OTHER REPORTS

When creating reports, always try to use a link within your report to provide drill-through capability. Drill-through permits the person viewing the reports to dive deeper into a particular item within the report. You can provide users a link to Computer Details so they can get more details on that particular computer, or you can link them to another report so they can get more information on other areas within Configuration Manager.

Cloning a Report

You might often want to tweak one of the reports already within your system but keep the existing report untouched. The best way of achieving this goal is to simply clone a report and then modify the clone, keeping the original report untouched so you can use it at a later date.

Cloning one of the built-in reports is also a very handy way to practice how to create reports. To clone a report, follow these steps.

- 1. Open the Configuration Manager console and expand Site Database.
- 2. Expand the Computer Management node, followed by the Reporting node and then the Reports node.
- 3. Choose the report you want to clone.
- **4.** Right-click the report and choose Clone from the All Tasks menu.
- **5.** Input the name of the new report and click OK.

Importing and Exporting Reports

One of the fastest and easiest ways to build reports into your Configuration Manager console is to import them from others who have already created the report you want. This technique allows administrators to share reports quickly and easily.

For example, myITforum.com has many reports that other administrators have uploaded in order to share their works with others. You can download reports from other administrators on myITforum.com. Use the following steps to import a report using the Import Wizard:

- 1. Open the Configuration Manager Administrator console and expand the Site Database
- **2.** Expand the Computer Management node, followed by the Reporting node.
- **3.** Right-click the Reports node.
- **4.** Choose Import Objects to launch the wizard shown in Figure 11.17.

Note that if you try to import a query, the Import Wizard will import the query but will place it under the Query node, not the Reports node.

- 5. In the Import Object Wizard, browse to the MOF File Name dialog box, shown in Figure 11.18, select Browse, and select the MOF file you want to import.
- 6. Select Next.
- 7. Ensure that you have the correct information by reviewing the name and information about the report, and select Next.
- **8.** Confirm that the description is what you are expecting and select Next.
- 9. Select Finish on the Completed Successfully page.

FIGURE 11.17 Import Object Wizard Welcome

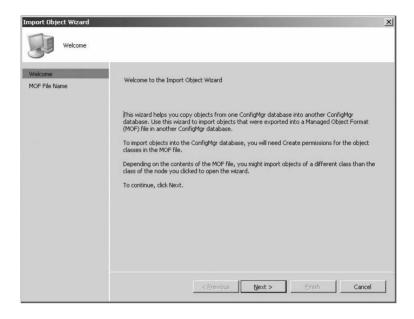
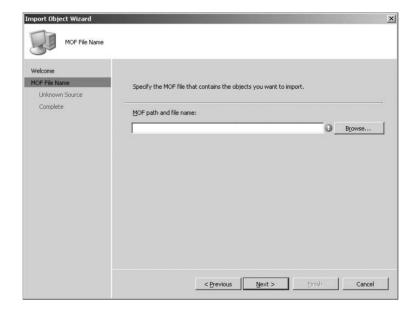


FIGURE 11.18
Browse to import MOF



Creating and Managing Security on Reports

As you begin to build rich reports, you will need to achieve a thorough security plan in order to provide only the reports that are approved for each group or individual. That will take some planning, and this book cannot suggest every possible solution for security of reports or within Configuration Manager in general.

As you have seen with other components within Configuration Manager, the Reports Property object has both a class and instance security that can be configured. This is very important to remember when you are designing your security for reports.

You can assign rights to all reports as a whole or to individual reports. You can assign the following rights to reports:

Administer Ability to assign rights and administration on the object.

Create Ability to create new reports.

Delegate Grant rights to the report.

Delete Delete the report.

Manage Folders Create, modify, and delete folders under the Reporting node.

Modify Make changes to the Report.

Read View the Report.

For an individual or group to be able to view a report, they must have the Read right at a minimum.

Basic SQL Commands

So far in the chapter you've seen how to create a new report from the console's New Report Wizard and how to import a report. The other option is to define the report using SQL scripting. This, of course, requires you to know the relevant SQL commands. In general, an understanding of SQL syntax is a huge asset for a Configuration Manager administrator, but not a requirement. However, within the scope of this book, we cannot cover SQL commands in depth. We suggest reading up on basic SQL commands so you can create very rich and powerful reports. Another way to learn is by simply opening existing reports and seeing how they are written.

Although we cannot cover every topic within SQL programming such as how to define queries to achieve rich reports within Configuration Manager, it will be useful to cover basics such as ORDER BY, sorting with DESC and ASC, COUNT, and setting header names using AS.

For all the examples we will be using the same report statement, shown here:

SELECT count(model0) as Count, Model0, Manufacture0 from v_gs_Computer_system GROUP BY ModelO, ManufacturerO ORDER BY count DESC

One way to make the presentation of reports look professional is to sort the items in some fashion. Within SQL you can use the following command to sort your reports:

ORDER BY count DESC

ORDER BY is the command that tells SQL to sort based on the column COUNT in this example. The order in which the items will be sorted is DESC, or descending. You can use ASC to sort ascending.

If you want to sort on multiple items, just add them to the list in the order in which you want to sort. For example:

```
ORDER BY count, ModelO DESC
```

Many times you will be tasked with showing very concise reports in which the end user just wants to know "How many units of model X do we have in our organization?" This is easily achieved by using the COUNT command.

```
SELECT count(model0)
```

This will show the count of the item ModelO in your report.

Many times, you will not want to have a report with column headings such as Model0, Manufacturer0, and so on. You will want to display meaningful header names. So the following example shows how to achieve this naming.

```
SELECT count(model0) as Count, Model0 as 'Computer Model', Manufacture0 as 'Manufacturer'
```

By adding the word AS into your SQL statement, you can specify the name of the column header. If the name contains a space, then you have to use a single quote.

CREATING A REPORT WITH SPECIFIC SECURITY ASSIGNED

As the Configuration Manager administrator, you will get various requests to generate reports to provide upper management with specific data they need. You will get requests similar to the following.

George T. Management wants to know how many laptops are in the organization, and he wants no one outside the IT Department other than himself to be able to view this report. To create that report, follow these steps:

 Browse to the Reports and select New Report. On the General tab, name the report "Laptops within the Organization." Click on Edit SQL Statement and input the following SQL statement:

```
SELECT TOP 100 PERCENT v_GS_WORKSTATION_STATUS.LastHWScan AS 'Last HW Scand Date',
v_R_System.Name0 AS 'PC Name', v_GS_NETWORK_ADAPTER_CONFIGUR.IPAddress0
AS IP,
v_Site.SiteName AS 'Site Name', v_GS_COMPUTER_SYSTEM.Manufacturer0 AS Manufacturer,
v_GS_COMPUTER_SYSTEM.Model0 AS Model, v_GS_PROCESSOR.MaxClockSpeed0 AS 'CPU Speed', v_GS_X86_PC_MEMORY.TotalPhysicalMemory0 AS RAM,
v_R_System.Operating_System_Name_and0 AS 'OS Name',
v_GS_OPERATING_SYSTEM.CSDVersion0 AS 'Service Pack',
v_R_System.User_Name0 AS 'Last Logon User'
FROM v_Site v_Site INNER JOIN v_RA_System_SMSAssignedSites ON v_Site.SiteCode
= v_RA_System_SMSAssignedSites.SMS_Assigned_Sites0
RIGHT OUTER JOIN v_GS_SYSTEM ON v_RA_System_SMSAssignedSites.ResourceID = v_GS_SYSTEM.ResourceID
```

```
LEFT
                      v_GS_LOGICAL_DISK
                                               v_GS_SYSTEM.ResourceID
       OUTER
             JOIN
                                          ON
v_GS_LOGICAL_DISK.ResourceID
             JOIN v GS COMPUTER SYSTEM ON v GS SYSTEM.ResourceID
LEFT OUTER
v GS COMPUTER SYSTEM.ResourceID
LEFT OUTER JOIN v_GS_PC_BIOS ON v_GS_SYSTEM.ResourceID = v_GS_PC_BIOS
.ResourceID
LEFT OUTER JOIN v_GS_SYSTEM_ENCLOSURE
                                           ON v_GS_SYSTEM.ResourceID
v_GS_SYSTEM_ENCLOSURE.ResourceID
LEFT OUTER JOIN v GS OPERATING SYSTEM ON v GS SYSTEM.ResourceID
v_GS_OPERATING_SYSTEM.ResourceID
LEFT OUTER JOIN v GS PROCESSOR ON v GS SYSTEM.ResourceID = v GS PROCESSOR
.ResourceID
LEFT
       OUTER
              JOIN
                     v GS X86 PC MEMORY
                                          ON v_GS_SYSTEM.ResourceID
v GS X86 PC MEMORY.ResourceID
LEFT OUTER JOIN v_GS_WORKSTATION_STATUS ON v_GS_SYSTEM.ResourceID
v_GS_WORKSTATION_STATUS.ResourceID
LEFT OUTER JOIN v_R_System ON v_GS_SYSTEM.ResourceID = v_R_System.ResourceID
LEFT OUTER JOIN v_GS_NETWORK_ADAPTER_CONFIGUR_ON v_GS_SYSTEM.ResourceID =
v_GS_NETWORK_ADAPTER_CONFIGUR.ResourceID
WHERE (v GS LOGICAL DISK.SizeO IS NOT NULL) AND
(v_GS_LOGICAL_DISK.DeviceID0 = 'C:') AND
(v_GS_SYSTEM.SystemRole0 = 'Workstation') AND
(v_GS_NETWORK_ADAPTER_CONFIGUR.IPAddress0 IS NOT NULL and
v_GS_NETWORK_ADAPTER_CONFIGUR.IPAddress0 <> '0.0.0.0') AND
v_GS_PROCESSOR.GroupID = 1 and
v_GS_SYSTEM_ENCLOSURE.ChassisTypes0 IN ('8','9','10','14')
ORDER BY v_Site.SiteName, v_R_System.Name0
```

The following is a list of all the various Chassis types Configuration Manager recognizes.

DESCRIPTION	Түре
Other	1
Unknown	2
Desktop	3
Low-Profile Desktop	4
Pizza-Box	5
Mini-Tower	6
Tower	7
Portable	8
Laptop	9
Notebook	10
Hand-Held	11

DESCRIPTION	Түре
Docking Station	12
All-in-One	13
Sub-Notebook	14
Space-Saving Chassis	15
Lunch-Box	16
Main-System Chassis	17
Expansion Chassis	18
Sub-Chassis Sub-Chassis	19
Bus-Expansion Chassis	20
Peripheral Chassis	21
Storage Chassis	22
Rack-Mounted Chassis	23
Sealed-Case PC	24
Tablet PC	65

- 2. Click OK. Click Next on the General tab. Click Next in the Refresh settings because we will not be requiring this to refresh automatically.
- 3. In the Links Dialog box, use the drop-down and change the Link type from the default No Link to Link to Computer Details. This will then allow you to choose what column contains the Computer name. In this instance, column 2 is the column we will be using.
- 4. Click Next.
- 5. Because Mr. Management is requiring you to limit this report to just the IT Department and himself, you need to add him in the Instance Security Rights section on the Security tab. Click Finish.

Creating Dashboards

Dashboards are basically reports that are arranged on a single pane within a single page. Reports are the major items of the dashboard. Dashboards can consist of a mix of any of the reports within Configuration Manager, excluding reports that contain prompts. However, now that you know how to clone reports, you could remove any prompts from a cloned report to ensure that it would work within a dashboard configuration.

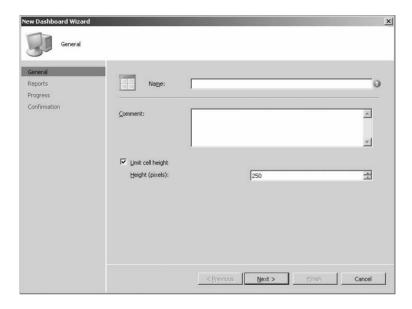
The same principles apply to dashboards as to reports. They can be e-mailed and set up as a favorite within your browser.

Follow these steps to create a dashboard:

- **1.** Open the Configuration Manager Administrator console and expand Site Database.
- **2.** Expand the Computer Management node, and then the Reporting node.
- 3. Right-click on Dashboards and click New Dashboard.

This will present you with the New Dashboard Wizard, shown in Figure 11.19.

FIGURE 11.19
The General page of the New Dashboard Wizard



You can limit the cell height of each Report within the Dashboard. The range is 50 pixels to 1500 pixels.

4. In the Reports dialog box, shown in Figure 11.20, specify the dimensions of the dashboard, and select the report(s) you want to appear in each cell of the dashboard. The rows and columns range from 1 to 5 each.

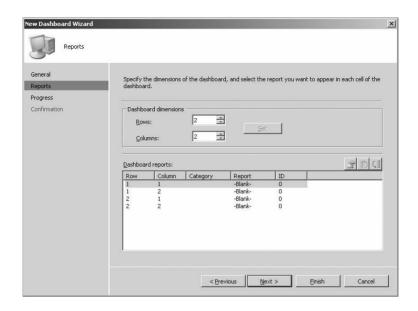
Add the reports you want to display and click Next.

5. Click Close in the Wizard Completion page.

Each report within the dashboard can be opened in a new window by clicking the link in its upper-left corner. This allows the end user to dive deeper into each report.

Dashboards do not have security options, but rather get their security rights from the reports they include. So, ensure the reports you are adding to the various dashboards have the appropriate security for each report or the end user will see an incomplete dashboard.

FIGURE 11.20 Specifying which reports to include in a dashboard



The Bottom Line

Set Up Reporting Point Roles Setting up the Reporting Point role within Configuration Manager allows not only administrators but everyone the ability to view reports in some fashion either via a CSV file or a direct link within the Web Reporting tool.

Master It What is the procedure to enable Reporting with Configuration Manager?

Create and Manage Reports Creating rich reports will provide you with a single place to get information about your Configuration Manager hierarchy and help you provide information about your environment in a few simple clicks.

Master It What are the steps to importing a report?

Create and Manage Security on a Single Report Creating rich security for reports will provide you with a great resource to limit which department or individuals can or cannot view individual reports.

Master It What are the steps to securing a report?

Create and Manage Dashboards Creating dashboards is a great place to get access to a lot of different data on one single pane.

Master It Create a custom dashboard that contains two reports.

Chapter 12

Desired Configuration Management

Using Desired Configuration Management, or DCM, you can easily configure a setting for clients and then check to ensure that each client has been configured as such. You'll do this in the Configuration Manager console by first creating *configuration items*, or CIs, that will specify a given setting as it should be configured. You'll then compile sets of CIs into *configuration baselines*, which define a complete baseline configuration that all clients in the group should conform to. Finally, you'll apply the baselines to a collection of Configuration Manager clients. Each client will then evaluate the baseline and, if it meets the baseline criteria, report back on its compliance with CIs in the baseline.

After reading this chapter you will be able to:

- ◆ Enable the DCM agent on your Configuration Manager clients
- Create DCM configuration items for a variety of settings
- ◆ Assemble DCM configuration baselines

Overview of Desired Configuration Management

At its simplest, Desired Configuration Management allows you to check your Configuration Manager clients to see if they are compliant with the settings you specify, but there is much more to it than that.

USERS ARE NOT CONFIGURATION MANAGER CLIENTS

While Configuration Manager allows you to easily create collections based on users and you can apply DCM baseline configurations to a collection of users, it is the agent on the computer that runs the compliance check and not the user.

What does that "more" consist of? Here are some of DCM's most powerful features and capabilities:

- ◆ The vast number of settings that you can check for compliance
- ◆ The capability to assemble configuration items into configuration baselines
- The capability to use regular expressions
- The capability to use scripts or .NET expressions when checking for compliance
- The capability to target an entire collection of computers with a configuration baseline but then specify a configuration baseline rule that applies only to a subset of those computers

- The capability to build your own categories of configuration items and the ability to search on categories
- The capability to nest configuration baselines and make them dependent
- The capability to build collections based on a Configuration Manager client reporting that it is not compliant and having a standing advertisement fix it

You may recall that this is not the first version of DCM; it was a feature pack that you could install as part of Microsoft's System Management Server 2003 SP1 (SMS 2003). A couple of years ago, one of the authors joined an instructor-led lab at the Microsoft Management Summit on creating DCM manifests. It was pretty crowded. After creating his second manifest file, our team member decided it was time to leave as the topic seemed far too complex. But turning around to leave, he noticed that of the 100+ seats, only a handful were still occupied. That's when he knew it wasn't just him; there was still some work to be done to get the technology to where it is today. Using DCM with SMS 2003 was quite the challenge; in Configuration Manager it has become much easier to use and is much more feature-rich, but the principle remains the same. This product has come a long way.

What Can You Do with Desired Configuration Management?

The best answer is that with DCM you can automatically check the compliance of your Configuration Manager clients against standards that you choose. Those standards can be company policies regarding how a computer is configured, policies for compliance with regulations such as Sarbanes-Oxley (SOX), or best practices defined by a vendor or based on your internal IT department's experience. They can be settings that a department manager has decided all the computers within their department must meet, or a means to identify computers that need more memory as defined by the IT manager in charge of desktops.

Given that range of potential applications, the next question is, what settings can you check for with DCM? This seems like an easy question to answer but of course it isn't. So, let's explore what you can and cannot do with DCM. First, DCM cannot allow you to get an extra hour of sleep every day. However, it can help create a baseline for your environment.

Let's examine this from a different perspective and then it will be clear what exactly you can and cannot check for using DCM.

Configuration Items

What are configuration items? As mentioned previously these are the standards that you assemble to create a configuration baseline, which is then applied to the Configuration Manager clients. There are specific types of configuration items that you can choose from to create these checks:

- Application CIs
- Operating system CIs
- Software update CIs
- General CIs

These checks are key to understanding the limits of what you can do with DCM. When you choose the type of configuration items using the wizard in the Configuration Manager Console, it will determine what types of checks you are allowed to include as part of a CI. Table 12.1 summarizes how the four CI types differ.

TA	BLE 12.1: Co	onfiguration Item Types	
	ТҮРЕ	DEFINITION	EXAMPLE
	Application	Used to check an application's settings for compliance	Checking Microsoft Office Word for the latest Normal.dot file
	Operating system	Used to check a particular operating system's version or settings for compliance	Checking to ensure that Configuration Manager clients have the latest service pack for Microsoft Windows Vista installed
	Software updates	Used to check Configuration Manager clients for software updates compliance	Checking the status of approved software updates on Configuration Manager clients
	General	Used to check settings of objects that do not fall under the other categories	Checking the hosts file to ensure that spyware has not modified the file or that the system has the latest hosts file

As you would expect, not all of these configuration item types offer the same properties. For example, the Operating System type contains a property to check for the exact build of the operating system that is running on the Configuration Manager client being evaluated; this option is not available in the other configuration types. As mentioned earlier, a configuration baseline can (and almost always will) contain multiple configuration items of all configuration types. The properties available to each configuration item type are listed in Table 12.2.

installed

TA	BLE 12.2: Pr	roperties of Configuration Item Types	
	Түре	Available	NOT AVAILABLE
	Application	General, Objects, Settings, Detection Method, Applicable, Security	Windows version
	Operating system	Windows version, Objects, Settings, Security	Detection Method, Applicable
	Software updates	General, Security	Windows version, Objects, Settings, Detection Method, Applicable
	General	General, Objects, Settings, Applicable, Security	Windows version, Detection Method

The reason for restricting configuration item types to specific properties, instead of having a single type with all properties available, is to keep the configuration items as small as possible. And defining configuration items as specific types allows you to reuse them when creating configuration baselines. For example, you can create an operating system configuration item that checks for Microsoft Windows Vista RTM.

Additional objects and settings are available when creating this configuration item type. You can also check for the presence of a specific file and its attributes. You can run validation against an assembly that is present, and you can even check the string value of a registry key and report on noncompliance for any of these objects or settings, all within the same configuration item. But if you design your configuration items with the idea of being able to reuse them in multiple configuration baselines, it is ideal if they are as lean and specific as possible. If you find that you need the configuration item to validate something else for a particular scenario, you can simply create a child configuration item. This configuration item will inherit all the original settings of the configuration item and allow you to add additional validations, leaving the original configuration item intact and not affecting any of the configuration baselines that are using that configuration item.

There are a few other items that we will briefly discuss below that are covered in more detail later in this chapter:

- When creating a new configuration item, the Software Updates type is not listed as an option. Software Update configuration items are not created in the same way as the other configuration items. Instead, they are added to a configuration baseline either when the baseline is created or later by editing the properties of the configuration baseline.
- Microsoft and other vendors make DCM configuration data available for download that contains configuration baselines or configuration items. Sometimes Configuration Manager cannot interpret all of the data contained and an icon will appear next to the imported configuration baseline or configuration item indicating this. The client will still read the imported data correctly when it checks for their compliance. You can find these packs at

http://technet.microsoft.com/en-us/configmgr/cc462788.aspx

Configuring Desired Configuration Management Client Agent Settings

Configuring the DCM client agent is as easy as checking a box and determining the appropriate schedule for clients to evaluate their compliance. Like all the other client agents in Configuration Manager, the DCM client agent is located in the Client Agents node. To navigate there in the Configuration Manager console, go to Site Database > Site Code - Description > Site Settings > Client Agents, and then in the right-hand console window locate the Desired Configuration Management Client Agent. Right-click on it and select Properties from the context menu. This will open the properties window for the DCM agent (see Figure 12.1). By selecting the box next to Enable Desired Configuration Management on Computers you enable the agent on all Configuration Manager clients. The default schedule for evaluation is set to a simple schedule of every seven days. You can adjust this schedule as necessary for your environment, including using a custom schedule that will allow more control over when it runs, but the default schedule is typically going to be adequate for most environments.

SETTINGS VS. OBJECTS

Settings and objects are not the same thing. When Configuration Manager was first released, the documentation on Microsoft's TechNet site regarding DCM was not as rich as it is now, and the Help file included with Configuration Manager didn't provide much more detail at the time. And there was some confusion regarding the difference between these settings and objects. In fact, if you read the descriptions of them on the TechNet site, they differed by only a few words.

Think of these terms literally. An object is a file, a folder, a registry key, and so on; and you can use DCM to check its settings or just whether it is present. For example, you might test the settings of the %System32%\drivers\etc\hosts file by checking whether it has the Read Only attribute set or whether its last modified date is equal to a specific date. An object is "physical"; it exists. A setting is a check against that object, like its last modified date or another attribute.

FIGURE 12.1
The DCM Agent



Creating Configuration Items

Configuration items are the pieces of the configuration baseline that, when assembled, will complete the puzzle and allow you to monitor configuration drift from what you have specified. To demonstrate the processes of creating configuration items and a configuration baseline, we'll use a utility called NightWatchman, described in the accompanying sidebar. Because there are so many ways to configure this product and to use it, you will be using it throughout this chapter so you can gain a better understanding of DCM and take these examples and apply them to any product you choose. NightWatchman also complements Configuration Manager well, so it is ideal for these examples. First you will set up configuration items to check the NightWatchman application to ensure that it is still configured as it was when it was deployed with Configuration Manager.

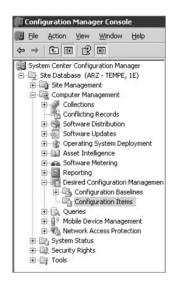
NIGHTWATCHMAN

A little history and information about NightWatchman are in order. NightWatchman is an application that allows you to shut down computers at a scheduled time, while also saving any data the user may have left open. It will also allow you to set and enforce the power scheme settings, such as when the monitor goes into standby, when the PC itself goes to standby, and so on. Another component of NightWatchman is reporting; it allows an administrator to report the make and model of the PC and

monitor, how many minutes the PC spends in each of the power states each day, and other pertinent information. NightWatchman also has three different shutdown modes: Passive, Active, and Forced. Passive means it will not process the shutdown if the user is logged in, Active means it will save any user data and then shut down the PC, and Forced is the same as active but without an option to postpone. All of these configurations, including the reporting, shutdown mode, and power scheme settings, are stored in the registry, and those are the settings you will build configuration items for and eventually assemble a configuration baseline with. If you do not have NightWatchman installed, you can download a free 30-day evaluation copy from the 1E website download section located at http://www.le.com/downloads. You'll need a copy installed if you want to try out this chapter's hands-on examples.

Start by opening the Configuration Manager console (if you ever close it). From the Site Database node, expand Computer Management > Desired Configuration Management and select the Configuration Items node. You should be in the location shown in Figure 12.2.

FIGURE 12.2The Configuration Items node



To create a new configuration item, you can either use the Actions tab on the right side of the Configuration Manager console, which some prefer not to display, or right-click the Configuration Items node and select New. Whichever method you prefer, your next choice will be to select the type of configuration item you are going to create. Notice that the types discussed earlier, minus Software Updates, are the available choices along with Folder and Search Folder. Choose Application Configuration Item to launch the wizard for the Application item type.

Name, Description, and Category

In the Create Application Configuration Item Wizard, you begin in the Identification tab. Fill in a Name and Description and then create a category before moving on to the next tab.

- 1. In the Name field, type 1E NightWatchman Scripts Folder Validation.
- 2. In the Description field, type This configuration item validates that the 1E NightWatchman scripts folder exists and that the Winword.vbs file is also in the folder.

- 3. Then, still in the Description field, press Ctrl+Enter to simulate a carriage return and add something descriptive stating who and when this was created or changed. You could use your initials or date or a combination; it just needs to be something that will help you later know who created or changed it and when, so that if anyone has a question about your configuration item, they know who to contact.
- 4. Click the Categories button to open the categories list. The list is populated with a few default categories and the top section will allow you to add your own custom categories.

WHAT IS A GOOD CATEGORY?

This will depend on your own administration style to a certain degree as well as the number of configuration items you will be creating. If you plan to check only Exchange servers for configuration drift, then you may not need any additional categories or just a few. If you plan on checking clients for application settings, Internet Explorer for configuration drift, different operating systems, files for the correct security settings, and so on, you would probably be wise to set up a standard for determining when new category types are needed, and when you can use existing ones. We have seen administrators who set up categories for every possible difference, and others who set up none. If you are going to use the categories and build a large number of configuration items and baselines, then you should set up custom categories, but don't go overboard; remember that categories are used to sort and search, so if you have too many, you get little or no benefit; too few is the same as none. It's best to use simple rules to create a standard: Does this configuration item fit into a category that exists already? Does that category generally and easily define this configuration item's purpose? If the answer is no to either, then a new category is probably needed.

For this example we are going to create a new category.

- **5.** In the Add A New Category section, type **1E** and click the Add button. This should add it to the Available categories section and select it. Before you click OK, verify that your categories look like Figure 12.3.
- **6.** Click OK to return to the Identification tab in the Create Application Configuration Item Wizard dialog, which should now contain the name, a description, and your newly created category. Verify that your dialog looks the same as Figure 12.4 and then click Next.

Choosing a Detection Method

The next tab in the wizard is Detection Method, which is unique to the Application configuration item type; it is not offered with the other types. The purpose of this tab is to specify the method used to verify that the application being checked for is installed on the client.

1. Three options are available. The first is "Always assume the application is installed." This will skip any verification check, which sounds great; you're essentially telling the system just to check the application for the settings you're about to specify. But if you do this while using certain rules in creating your configuration baseline, you will run into problems.

BASELINE RULES

Which baseline rules cause problems? You will need to decide which if any of the following: "If these optional application configuration items are detected, they must be properly configured," "These application configuration items must not be present," and "If another baseline is dependent on these configuration items it may invalidate your dependency."

FIGURE 12.3 Create Application Configuration Item Wizard Categories dialog box

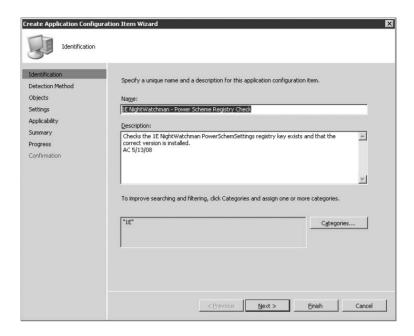
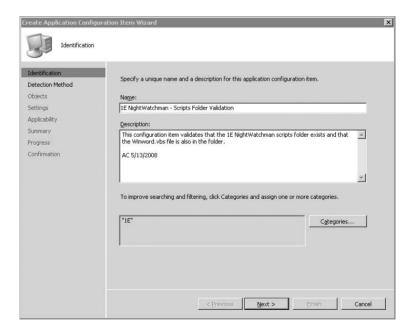


FIGURE 12.4Create Application Configuration Item Wizard

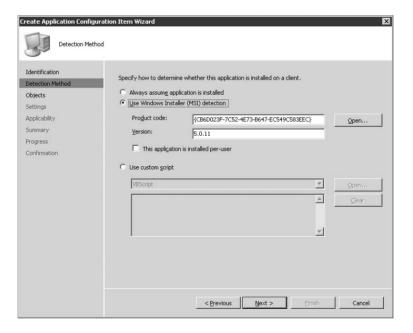


The second option is to verify the product code the application vendor included with the MSI installer and the version, as you are going to do in this example. The final option is to choose whether to use a script; you can use VBScript, JScript, or PowerShell.

- **2.** Select the Use Windows Installer (MSI) Detection radio button. This will require you to have access to the installation files, but if you downloaded the NightWatchman application from the 1E site, you should already have this file. If not, please download it now.
- Assuming you have the NightWatchman files downloaded and extracted, click the Open button in the Detection Method page and browse to the folder where you extracted the files.
- **4.** Find and click the NightWatchman.msi file, and it will populate the Product Code and Version fields in the Detection Method page.

If this application is installed on a per-user basis you may also need to check the corresponding box for it to be properly detected. If it was installed for all users, that is not necessary. Before moving on to the next step, creating and validating an object, verify that your wizard settings look similar to Figure 12.5. (Your product code and version number may be different.)

FIGURE 12.5
Cl Application Detection Method



5. If everything is in order, click Next to proceed to the Objects tab.

Creating and Validating an Object

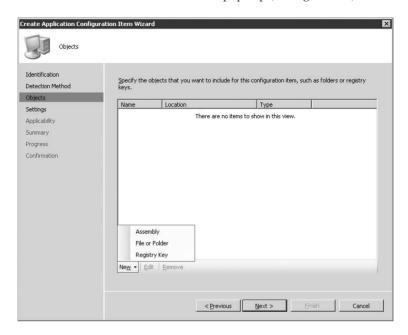
In the Objects tab, you tell the Create Application Configuration Item Wizard what type of object to look for and where that object lives.

CREATING AN OBJECT

In the empty window there are three columns: Name, Location, and Type, and a New button.

1. Click New and choose File or Folder from the menu that pops up (see Figure 12.6).

FIGURE 12.6 Cl Objects New menu



This opens the New File or Folder Properties window, shown in Figure 12.7. The General tab here has several fields and two drop-down menus. The red circles with exclamation points indicate that the blank fields require input before you can create the configuration item.

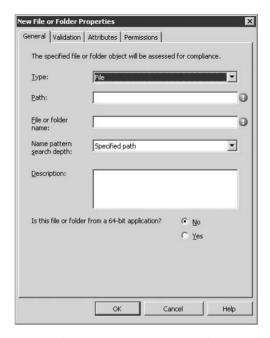
- **2.** Starting at the top, from the Type menu, select File.
- In the Path field, enter C:\Program Files\1E\NightWatchman50\Scripts and in the File Or Folder Name field, enter winword.vbs.
 - The winword.vbs script is run by NightWatchman during an Active logoff to save any of the user's data in Microsoft Office Word.
- 4. Leave the Name Pattern Search Depth option at the default Specified Path. The other two options require that you use wildcards when you specify the search path or in the file or folder name you are validating, depending on which search type you choose. You should verify that the folder path and file name on your client are still valid.

WILDCARDS AND ENVIRONMENT VARIABLES WITH DCM

The use of wildcards is allowed and actually required for the "Specified path (pattern)" search type as well as the "Specified path and all subfolders" search type. The ? and * characters are the permitted wildcards, but they should be considered and used carefully. Using wildcards can produce

additional overhead when you're trying to find a file or folder, as the search will work exactly as instructed. Specifying the Windows directory, for example, and then telling it to search all subdirectories is not ideal. You can also make use of environment variables such as %ProgramFiles% or %AllUsersProfile%. The result may be that you get more than one return result if the users all have the file or folder you are looking for in the search path.

FIGURE 12.7 New File or Folder Properties dialog box



- **5.** In the Description field, enter **This configuration item locates the file winword.vbs and validates that it is the latest version of this file on all NightWatchman clients**.
- **6.** You can leave the Is This File Or Folder From A 64-Bit Application radio button at the default of No for NightWatchman.

64 BIT APPLICATIONS AND THE REGISTRY

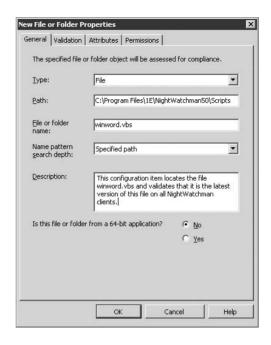
Readers who have 64-bit applications should be aware of a possible issue with the registry and configuration baselines: because of the "registry reflector" that mirrors certain registry keys for interpretability, it is possible that you could detect the presence of two registry keys with a single configuration baseline. If you are running 64-bit applications, you will need to check for this before deploying a configuration baseline containing a configuration item that involves checking for a registry key associated with a 64-bit application.

You have finished creating the object's details by telling DCM what you are looking for and where you want it to look for it. The next step is to validate the object by telling DCM the specifics of the object to validate.

7. Before you move on the Validation tab make sure your General tab looks like Figure 12.8.

FIGURE 12.8

New File Or Folder Dialog box completed



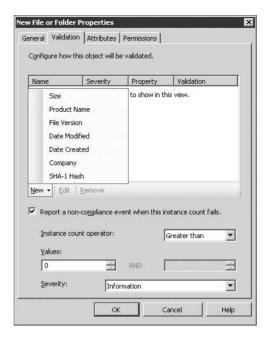
VALIDATING AN OBJECT

Now that you have created your object, you are going to tell DCM how you want this CI to validate the file. As you did when creating a new object, click the New button to get started, as shown in Figure 12.9.

- 1. From the context menu, choose Date Modified to open the Configure Validation window, where you will fill in exactly the validation criteria you are looking for.
 - In the Configure Validation window, there are again several more fields and drop-down menus, including a space to input the name value, with Date Modified supplied by default for convenience.
- 2. The top field is the name of the validation rule. This is a required field, and a value will be supplied by default. You are just going to remove the _New_Rule at the end of the default text, resulting in a rule name of File_winword.vbs_Date Modified.
- **3.** In the Description text box, enter the following or something similar but make sure you also put your initials and the date in the event someone else reviewing this rule has questions:

Validates that the winword.vbs file in the NightWatchman scripts folder has the latest version of the file approved and distributed by IT. 7/11/2008"

FIGURE 12.9
The Validation tab's
New menu button



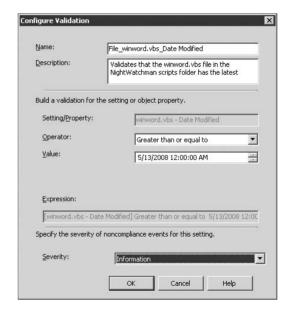
- **4.** In the Build A Validation For The Setting Or Object Property area of Configure Validation, you tell DCM exactly how to validate this file. The Setting/Property field is grayed out and unavailable because you have already selected the type of setting you are going to validate against. Below that is the Operator drop-down menu, where you have nine operators to choose from:
 - Between
 - ◆ Equals
 - Greater than
 - Greater than or equal to
 - Less than
 - Less than or equal to
 - None of
 - Not equals
 - One of

By choosing Between as the operator, you get the option to specify a range. In this example, choose the Greater Than Or Equal To operator and in the Value field enter the current date and leave the time at 12:00:00 AM. Obviously, because you are going to use this as a test, you should make a change to the file so that the modified date is not its original or input that as your validation date and time.

- 5. In the bottom section of Configure Validation, you choose the level of severity should this check fail on one of your Configuration Manager clients. There are four levels to choose from here:
 - ◆ Information no Windows event message
 - **♦** Information
 - Warning
 - Error

All four levels report back to Configuration Manager, but the first one does not write an event to the application event log in Windows as the other three do. This was made an option to prevent DCM validations from filling up the event logs on clients if a check comes back as invalid too many times. This might happen if, for example, you input the wrong validation data or if something out of your control, such as an upgrade or service pack installation, makes the validation check no longer return TRUE. In this exercise, select Information if you don't already have it selected and then verify that your window looks like Figure 12.10 before clicking OK to continue.

FIGURE 12.10
The Configure Validation window



6. You'll return to the New File or Folder Properties window, where listed in the formerly empty section you'll now see the new validation rule for this file. You now have to tell DCM if you want it to report on a noncompliant event and, if so, the details of when and how it should report.

The Report A Non-Compliant Event When This Instance Count Fails check box should already be selected. This option turns on and off the reporting of a noncompliant DCM client and allows you to set the severity of noncompliance as well as at what point it should report. Next to Instance Count Operator, you have the same drop-down menu selections

- as the Configure Validation window, and these same nine options are available with other configuration item types.
- 7. You are going to use the Greater Than operator in this case. Leave the Value and Severity to their defaults as well, which results in a compliance rule that will report when a DCM validation check fails at least once and will report as an informational severity. In this example, we have left the Severity settings at their defaults. Later in this chapter, you will see how different severity levels combine with other settings during the reporting.

ATTRIBUTES AND PERMISSIONS

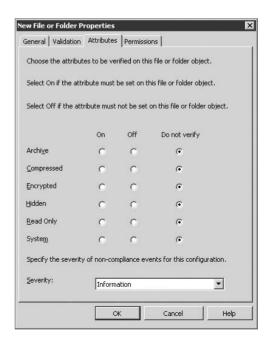
There are two additional tabs in the New File Or Folder Properties window that you do not use in this example: Attributes and Permissions. They are certainly worth knowing about and are great options for additional validation or in place of the validation you are using in this example. Here's a quick tour of the options so that you can make use of them in your own configuration items.

- First click the Attributes tab. The attributes are as you would expect them to be; they are
 the standard file attributes that have been around since the DOS days with a couple of new
 additions to the list:
 - archive
 - compressed
 - encrypted
 - ♦ hidden
 - read only
 - system
- **2.** Each attribute has three radio buttons that enable you to tell the configuration item whether the attribute should be enabled or disabled in the file or folder or to skip the verification altogether. If you choose the On or Off radio button next to any of the attributes listed, it will validate that the file or folder specified has that attribute enabled or not. The default is Do Not Verify for all the attributes, and for this example leave them at the default.
 - Below the attributes, you have the ability to choose the level of severity reported if you choose to check for any or all of these attributes and the validation returns noncompliance. This would make a good validation if, for example, you distributed a hosts file to your clients and wanted to make sure that the file was set to Read Only still as a method to check for possible spyware altering this file. See Figure 12.11 for a view of this tab.
- 3. Click the Permissions tab. On this tab you can specify what NTFS permissions the selected file or folder should have set, and you can choose whether those should be the only permissions set or whether there are additional users and groups with permissions as well. The available options for the types of permissions you can check for are all-inclusive, including those you would see listed in the available permissions when setting special permissions on a file or folder.
 - If you do check for permissions, the user or group entered must be entered in the NT4 format of <code>domain\user</code> not the <code>user@domain</code> style. Also note that when you choose some permissions, others will be selected by default for you and others disabled. If you select

Full Control but then clear the Read check box, Full Control is removed as well. You can check for the following:

- ◆ Full control
- ◆ Read
- Write
- Execute
- ◆ Transverse folder or execute file
- ◆ List folder contents or read data
- Read attributes
- Read extended attributes
- Create files or write data
- Create folders or append data
- ♦ Write attributes
- Write extended attributes
- ◆ Delete subfolder and files
- Delete
- Change permissions
- ◆ Take ownership
- Read permissions

FIGURE 12.11 New File or Folder, Attributes tab

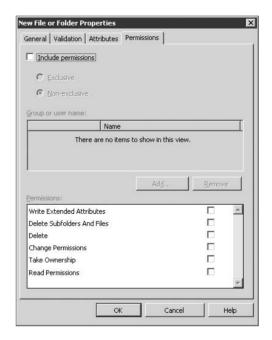


4. If you find that you need to reset the permissions you have chosen and don't want to remove all of the options you have entered, simply clear the Include Permissions check box. It will remove all the users and groups along with the chosen permissions and return the tab back to its default settings. (Make sure you don't use the Cancel button, as it will cancel all of the settings you have entered on all the tabs of the window, not just the Permissions tab!) Figure 12.12 shows the Permissions tab as it first appears.

FIGURE 12.12

New File or Folder,

Permissions tab



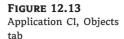
5. You have now created your first configuration item. After reviewing your settings on the General and Validation tabs, click OK at the bottom of the New File Or Folder Properties dialog box.

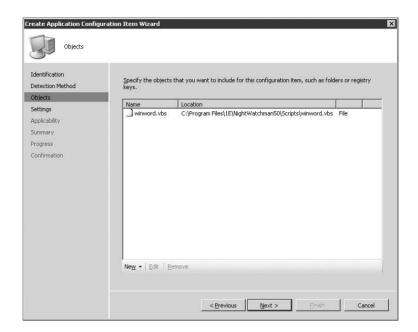
COMPLETING THE NEW CONFIGURATION ITEM

After clicking OK at the end of the previous section, you should be back at the Create Application Configuration Item Wizard window, with the new configuration item object listed, as shown in Figure 12.13.

This is the only object and validation you are going to create in this first example, but other tabs and their options will be covered in the examples to follow, including Settings and Applicability.

- Because you are not going to make any additions to this configuration item, you can click through to the end using the Next button at the bottom of the window or by clicking through the tab located on the right side of the window.
- **2.** Eventually you should reach the Summary tab, which will give you a list of all the options and settings selected while creating this configuration item. Verify that these are as you expect them to be; if any are not, use the Back button or the tabs to make any modifications.





3. Once you have checked to ensure that everything is in order, click the Next button or the Progress tab to start the process of building the configuration item. See Figure 12.14 for the details of the Summary page.

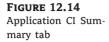
After a short period, the progress indicator and window should disappear and you should now see the Confirmation window, which says

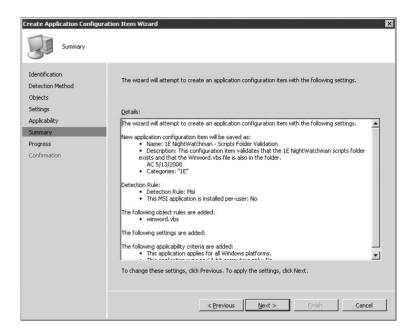
Success: You have successfully completed the Create Application Configuration Item Wizard with the following settings

along with a list of the settings you chose. Verify again that everything is listed as expected and you can now click the Close button to complete the wizard and return to the Configuration Manager console.

Parent and Child Configuration Items

You now have a configuration item that will check to see if your application is installed. It will also check to ensure that you have the most up-to-date script for saving the user's data when he or she leaves Microsoft Office Word open at the end of the day and the NightWatchman application shuts the computer off at its scheduled time. In this next example, you continue to use the NightWatchman application and its settings, but this time you will check the registry values to make sure that the client is scheduled correctly, all while building child configuration items that inherit the settings of the parent. This will save you some time and prevent human error by not forcing you to enter the same settings each time.





CREATING A PARENT CI

To set the scene, let's go over the behavior you should expect to see your NightWatchman application perform. Then you will build the CIs to check the configuration of the application on your clients. The 1E NightWatchman application should be configured as follows:

Log Off Action – Active This logs the user off and saves his work at the scheduled shutdown time.

Shutdown Action – Normal This turns the computer off after shutdown instead of putting it into a low power mode such as standby or hibernate.

Shutdown Hour – 19 7:00 p.m. is the scheduled shutdown time.

Countdown Seconds – 60 The setting will control how long the counter runs and displays the dialog box to the user before initiating the shutdown sequence.

Retry Attempts – 3 If the user is at her desk and the countdown to shutdown starts, she has the option to click the Postpone button to prevent the shutdown. This setting indicates how many times NightWatchman will try again to start and finish the countdown and begin the shutdown process.

Retry Interval – 60 Combined with the Retry Attempts settings, this controls how long before the dialog box appears on the screen again; in this case it is every hour.

These settings, in summary, mean that at 7 p.m. the NightWatchman application will present a dialog box on the screen with a 60 second countdown. If the user is working late, he can click the

Postpone button and the dialog box will go away; then again at 8 p.m., the dialog box will prompt the user just as before. If the user clicks Postpone again, the warning will come back at 9 p.m., and then at 10 p.m. At 11 p.m. it will make its final attempt and, assuming the user is done working by then, when the counter expires NightWatchman will save any work the user left open, log the user off, and then shut down the computer gracefully for the night.

Now let's build the required CIs to check all of this:

- Back in our Configuration Manager console under the DCM node, make sure you have the Configuration Items folder selected. Right-click it and select New and then Application Configuration Item.
- **2.** On the General tab, enter the following settings:

Name: 1E NightWatchman - Log Off Action Active

Description: Configuration item for 1E's industry leading PC power management tool.

Categories: 1E

3. On the Objects tab, select New Registry Key from the menu and enter or choose the following settings:

Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\1E\NightWatchman50

Is this registry key associated with a 64-bit application: No

Report a noncompliance event when this instance count fails: Yes/Checked

Instance operator: Greater than

Values: 0

Severity: Warning

- **4.** On the Settings tab, choose New Registry from the menu.
- **5.** On the General tab of the new registry validation, enter the following settings:

Display name: Active Log Off Action

Description: Checks that the log off action of 1E's NightWatchman client is correctly configured to allow an Active log off.

Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\1E\NightWatchman50

Value name: LogOffAction

Is this registry key associated with a 64-bit application: No

6. On the Validation tab of the new registry validation, choose

Data type: String

and click New on the menu in the Details pane.

7. In the Configure Validation window displayed after you click New, enter or choose the following settings:

Name: Log Off Action = Active

Description: LogOffAction value is correctly set to Active.

Operator: Equals
Value: Active
Severity: Warning

8. Click OK to return to the Validation tab of the new registry validation and choose the following settings:

Is this registry key associated with a 64-bit application: No

Report a noncompliance event when this instance count fails: Yes/Checked

Instance operator: Greater than

Values: 0

Severity: Warning

- **9.** Click OK to save your changes to the Settings tab and move on.
- **10.** On the Detection Method tab, select the radio button Always Assume Application Is Installed.
- 11. On the Applicability tab, make sure the All Windows Platforms radio button is selected.
- **12.** Review your settings on the Summary tab and when you are confident everything is correct, click the Next button, which after a brief intermission should get you to the Confirmation tab indicating the CI was created successfully.
- **13.** Back in the Configuration Manager console, still viewing the CI folder, you should now have a new application CI with the name 1E NightWatchman Log Off Action Active.

CREATING CHILD CIS

You will go through the same process to create five child CIs from this one, and when you are done, you will assemble the Configuration Baseline that you can then apply to collections to interrogate your clients with and determine if they are compliant.

The first child CI you are going to create is Countdown Seconds.

- In the Configuration Manager console, right-click the new 1E NightWatchman configuration item you just created and select Create Child Configuration Item. This will start the wizard.
- 2. On the General tab, enter the following

Name: 1E NightWatchman - Log Off Action Active - Child - Countdown Seconds

Description: Configuration item for 1E's industry leading PC power management tool

The Object tab is grayed out; it inherits its settings from the parent CI.

3. The Settings tab has two main areas, General and Validation. In the General area, enter the following settings:

Display name: CountdownSecs = 60 Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\1E\NightWatchman50

Value name: CountdownSecs

- 4. In the Validation area of the Settings tab, for Data Type, select Integer.
- 5. Click New on the menu in the Details pane and enter or select the following settings:

Name: $Registry_CountdownSecs = 60$

Operator: Equals

Value: 60

Severity: Information

- **6.** Click OK to return to the Validation tab of the new registry validation.
- 7. In the Settings area of the Validation tab, choose the following:

Report a NonCompliance Event When This Instance Count Fails: Checked

Instance Operator: Greater than

Values: 0

Severity: Information

8. Click OK to save your changes to the Settings tab and move on.

Notice that both the Detection Method Applicability tabs of the wizard are grayed out; they inherit their settings from the parent CI.

On the Summary tab, verify that your settings are correct and then create your CI. Once the process is complete, you will again get the confirmation window and you can close the wizard.

You now have your first child CI. This process should have taken you only a few minutes now that you are starting to get the feel for the wizard and its flow, including where everything is. To follow along with this chapter's complete example and compile a set of configuration items into a configuration baseline, repeat the process just outlined to create the remaining child CIs: Retry Attempts, Retry Interval, Shutdown Action, and Shutdown Hour. Most of the settings are the same for each item.

1. For Retry Attempts, start by entering the following:

Name: 1E NightWatchman - Log Off Action Active - Child - Retry Attempts

Description: Configuration item for 1E's industry leading PC power management tool

Display Name: Retry Attempts
Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\1E\NightWatchman50

Value Name: RetryAttempts

- **2.** In the Validation area of the Settings tab, for Data Type choose Integer.
- 3. Click New on the menu in the details pane and enter or select the following:

Name: Registry_Retry Attempts = 3

Operator: Equals

Value: 3

Severity: Information

4. Click OK to return to the Validation tab and set the following:

Report a NonCompliance Event When This Instance Count Fails: Checked

Instance Operator: Greater than

Values: 0

Severity: Information

5. Click OK to save your changes to the Settings tab and move on to create the next child CI.

The next CI is for Retry Interval.

1. Start by entering the following:

Name: 1E NightWatchman - Log Off Action Active - Child - Retry Interval

Description: Configuration item for 1E's industry leading PC power management tool

Display Name: Retry Interval Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\1E\NightWatchman50

Value Name: Retry Interval

- **2.** In the Validation area of the Settings tab, for Data Type choose Integer.
- **3.** Click New on the menu in the details pane and enter or select the following:

Name: **Registry_Retry Interval** = **60**

Operator: Equals

Value: 60

Severity: Information

4. Click OK to return to the Validation tab and set the following:

Report a NonCompliance Event When This Instance Count Fails: Checked

Instance Operator: Greater than

Values: 0

Severity: Information

5. Click OK to save your changes to the Settings tab and move on to create the next child CI. Next you will create the Shutdown Action CI.

1. Start by entering the following:

Name: 1E NightWatchman - Log Off Action Active - Child - Shutdown Action

Description: Configuration item for 1E's industry leading PC power management tool

Display Name: **Shutdown Action** = **Normal**

Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\1E\NightWatchman50

Value Name: ShutdownAction

- 2. In the Validation area of the Settings tab, for Data Type choose Integer.
- 3. Click New on the menu in the details pane and enter or select the following:

Name: Registry_Shutdown Action = Normal

Operator: Equals Value: Normal

Severity: Information

4. Click OK to return to the Validation tab and set the following:

Report a NonCompliance Event When This Instance Count Fails: Checked

Instance Operator: Greater than

Values: 0

Severity: Information

5. Click OK to save your changes to the Settings tab and move on to create the final child CI.

The last child CI before you make your Configuration Baseline is Shutdown hour, which defines the time when the first attempt to shut down the computer occurs.

1. Start by entering the following:

Name: 1E NightWatchman - Log Off Action Active - Child - ShutdownHour 19

Description: Configuration item for 1E's industry leading PC power management tool

Display Name: **Shutdown Hour** = 7 PM

Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\1E\NightWatchman50

Value Name: ShutdownHour

2. In the Validation area of the Settings tab, for Data Type choose Integer.

3. Click New on the menu in the details pane and enter or select the following:

Name: Registry_Shutdown Hour = 7 PM

Operator: Equals

Value: 19

Severity: Information

4. Click OK to return to the Validation tab and set the following:

Report a NonCompliance Event When This Instance Count Fails: Checked

Instance Operator: Greater than

Values: 0

Severity: Information

5. Click OK to save your changes to the Settings tab.

And that is the last one! Let's get that baseline created.

Building a Configuration Baseline

Now that you have amassed all the puzzle pieces and turned them right side up, let's put them all together to make it look like the picture on the box. You have built the configuration items to make your configuration baseline, which is what you assign to your clients to check for drift.

Briefly, you have a parent configuration item with five child configuration items that validate your NightWatchman settings for a 7 p.m. shutdown with the retry interval set at 60 minutes, the number of retries set to 3, the countdown set to 60 seconds, and the shutdown action set to normal; and the parent CI will validate that the client is configured for an active logoff. You also created a CI that would check to see if the winword.vbs file was up-to-date and present on your clients.

Creating the Initial Baseline

As it does with most tasks, Configuration Manager provides a wizard to guide you in creating a configuration baseline.

- 1. To navigate to the DCM Configuration Baseline folder, expand Site Database ➤ Computer Management ➤ Desired Configuration Management, and click Configuration Baselines. As usual, you can either click the New Configuration Baseline link in the Actions pane or simply right-click on the Configuration Baselines folder on the left and select New Configuration Baseline. (We prefer right-clicking, as there is less mouse movement.)
- 2. You should now see the Create Configuration Baseline Wizard, shown in Figure 12.15. The first tab that you see is the Identification tab, familiar from the wizard for creating the

configuration items. Here you select the categories and input the name and description. Fill in the following details.

Name: 1E NightWatchman - Active log off and winword script check

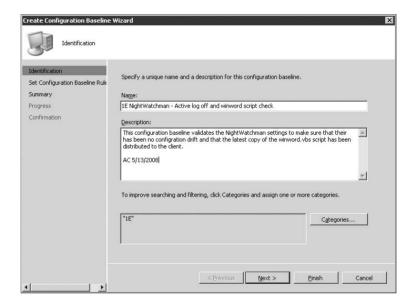
Description: This configuration baseline validates the NightWatchman settings to make sure that there has been no configuration drift and that the latest copy of the winword.vbs script has been distributed to the client.~LB~LBAC 5/13/2008

Categories: 1E

To select 1E as the category, first click the Categories button to display a list.

3. Verify that your settings match those shown in Figure 12.15 and click Next.

FIGURE 12.15
Configuration Baseline
Wizard, Identification
tab

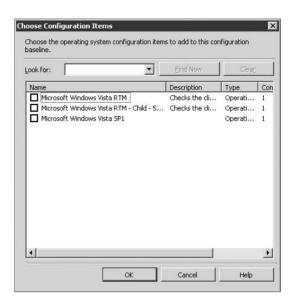


On the next tab, you are going to select rules and then the configuration items you want to include with those rules. This process is quite different from the way you build configuration items, so we will explain it in a little more detail.

Baseline Rules

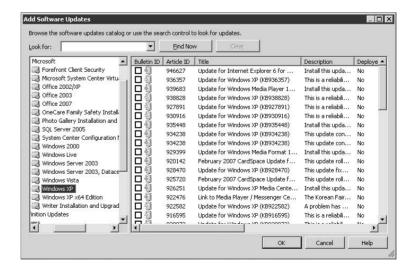
The process of creating rules is similar to the manner in which you build rules in Outlook. Or think of it as telling DCM a story or writing a recipe to build your baseline. The available rules include defining what operating system you want to check for, but this is not a substitute for the configuration item's Applicability tab, where you get a list of all the different operating systems and service pack level. If you have not built a configuration item to check for a specific operating system, when you click the link in the rule there will be no configuration items to choose from and nothing to put into this rule. Although our example doesn't include them, Figure 12.16 illustrates the further selections available when you have also created one or more operating system CIs. In this case, there is one CI to check for Microsoft Windows Vista RTM and one for Vista SP1.

FIGURE 12.16
Choosing Configuration
Items



Another available rule is Checking For Software Updates. Earlier in the chapter we mentioned that you cannot create CIs for software updates in the same location as the other CI types and you must specify them when creating your configuration baseline; this is exactly where you would specify the software updates to check for. If you click the link in the software update rule, it will spawn a new window called Add Software Updates (see Figure 12.17), where you will see the same folder display as in the Configuration Manager console and you will have all the updates that you set to download to your server available to choose from. It is important to understand that you will not see software updates that you may have already added to the baseline. You can see the software updates that are included in this configuration baseline by viewing its properties in the Configuration Manager console.

FIGURE 12.17Adding Software Updates



Another rule that can be built is Configuration Baselines. This is how you would use other configuration baselines that you have created and thus save you quite a few steps. Clicking on this also opens another window that lists the configuration baselines previously created and available to select, much like Figure 12.16.

We have saved the other three rules for last because they are all related to application CI types, differing in the way that they build the rules of your baseline:

- Applications and general CIs that are required and must be properly configured
- Optional application CIs that if detected must be properly configured
- Application CIs that must not be present

Let's consider how each of these might be used when building a configuration baseline.

APPLICATIONS AND GENERAL CIS THAT ARE REQUIRED AND MUST BE PROPERLY CONFIGURED

This rule means that if you select an application CI, it will use the detection method specified to ensure that the application is installed. We used two different detection methods when we built the application CIs for our NightWatchman. For the first one, we pointed it at the MSI file and got the version and GUID, and for the last set of parent and child CIs we told it to always assume the application was installed. When we build an application CI and use the "always assume installed" detection method, we are simply skipping the detection method. Thus, there is no chance that the detection method will fail and the next step in our application CI will do its check. Once a CI fails a check, the remainder of the CI checks, whether settings or objects, are not validated against the client. The actual status returned can vary depending on these settings as well; if the Detection method is specified and fails, it will return a Not Detected compliance.

You would use this to add general CIs to your list of rules, but also for applications that you want to ensure are installed, or at least to detect that they are installed, and that they are configured correctly. Going back to the CIs we created for NightWatchman, if we specified the CIs that detect if the latest winword.vbs file is on the client, the CI for NightWatchman would first have to pass the detection method we also specified, so if the version or GUID returned noncompliant, then the rest of the CI validation would be skipped and we would get a status message indicating that the application was not detected.

IF OPTIONAL APPLICATION CIS ARE DETECTED, THEY MUST BE PROPERLY CONFIGURED

The rule that if optional application CIs are detected they must be properly configured means that if you make application CIs part of the baseline and they fail to be detected, then the validation checks that are part of that CI will be skipped; if the application is detected, it will then validate the objects or settings specified in the CI and report compliance or noncompliance. A typical use for this type of rule might be a situation in which you are not sure an application is installed on the client, but in the event that it is, you want to make sure that the application is configured correctly.

SELECTED APPLICATION CIS MUST NOT BE PRESENT

The last application CI rule specifies that selected application CIs must *not* be present. This type of rule could be used to make sure that an application is not present on a system. For instance, if you are checking the configuration of NightWatchman 5.x, you might want to make sure that NightWatchman 4.x was properly removed. Assuming you had a baseline that you used to check

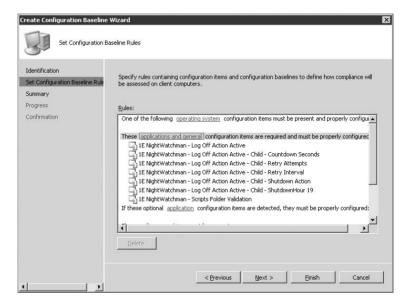
the configuration of NightWatchman 4.x, you could select one of them and have it run to validate that the application had been previously uninstalled.

Add CIs to the Configuration Baseline

Now that you have seen the different rules and how they are used, you can return to the running example and add your CIs to the baseline.

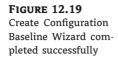
- Begin by selecting the rule "These Applications And General Configuration Items Are Required And Must Be Properly Configured."
- 2. When the Choose Configuration Items window opens, select all the NightWatchman configuration items by selecting their boxes. This is where having custom categories can come in handy; not only are they listed but, as you can see, you can search on them as well, greatly streamlining selection if you had hundreds or thousands of CIs to choose from.
- **3.** After you have selected the CIs, click OK to return to the previous screen. You should now see the CIs you selected listed directly under the rule you chose, just as in Figure 12.18.

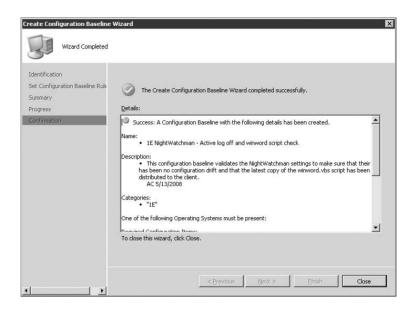
FIGURE 12.18
Set Configuration
Baseline Rules



- After validating that you have the correct CIs added to the appropriate rule, click Next to move to the Summary tab.
- **5.** Check that what is listed on the Summary tab is in line with what you have entered in the baseline rules and once you are confident everything is in order, click Finish. In just a couple of seconds you should see the Confirmation tab indicating that your configuration baseline has been created successfully (see Figure 12.19).

You can now click the Close button and return to the Configuration Manager console, where you will next assign your new configuration baseline to clients that will be evaluated for compliance.

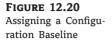


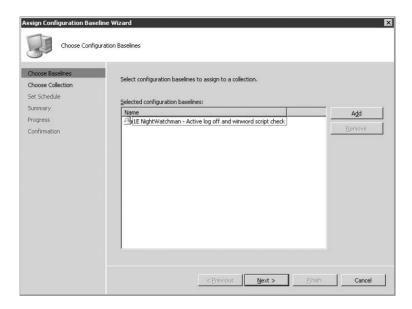


Assigning the Configuration Baseline to Clients

Now that you have all the baselines configured, you need to assign them to the clients or all your hard work is not being used. Assigning the Configuration Baselines to the clients will allow Configuration to monitor the clients and ensure the baselines are met.

- 1. Back in the Configuration Manager console, you should still see the configuration baselines. If you highlight the newly created baseline, you will see its details at the bottom of your console. To assign this configuration baseline to clients for validation, right-click on the baseline and choose Assign To A Collection. This will start the Assign Configuration Baseline Wizard, shown in Figure 12.20.
 - This should prepopulate the selected configuration baseline that you used to launch the wizard; as you can see, you can add or remove additional configuration baselines by using the Add and Remove buttons on the left.
- At this time if you see the correct configuration baseline, click the Next button at the bottom of the window.
- 3. The next tab is Choose Collection, where you are going to select a collection to assign this baseline to. Do that now by using the Browse button. Be sure to select a collection that includes the clients where you have installed and configured the NightWatchman client. After you have selected the appropriate collection, click the Next button to move on to the next tab.
 - The final tab where you make settings is Set Schedule. Here you set the validation schedule, much as you do with an advertisement. You can create a simple schedule such as Run Every 7 Days or create a custom schedule for more flexibility.
- **4.** For the example, use the custom schedule and set it to reoccur every hour; this ensures that you get the validation to run and return data so you can examine the reports.





- **5.** After you have specified the schedule, click Next to go to the Summary tab where you can review the settings prior to making the changes.
- **6.** After reviewing the settings, proceed to assigning the baseline by clicking Next once more. And after just a few seconds you should see the Confirmation tab appear, indicating that the assignment has been completed successfully. You may now click the Close button.

Additional Configuration Baseline Options

Within the Configuration Manager console, there are some additional options available while viewing the configuration baseline folder. If you have the Actions pane visible, you should see the option to Import Configuration Data. This option allows you to import a .CAB file that could have been created by a vendor, using an external tool such as CP Studio 2008, or from another Configuration Manager site. If you have a baseline currently selected you should also see some additional options, including the ability to export configuration data. This will allow you to export your data, so that you can import it to another site or edit it with an external tool.

You can also duplicate the baseline. For example, if you needed to make a copy but wanted to make small changes to it, such as adding an additional operating system rule, this would be a quick method to accomplish that without your having to re-create the entire baseline and specify the same rules again.

You also have the ability to disable the baseline; if you select this option it will stop the clients from evaluating this baseline. Once a baseline is disabled you have the option to enable it from the same location on the Actions pane. You can also view the XML that defines this baseline by clicking the View XML Definition button. The Manage Categories option should be pretty self-evident at this point; you can add or remove categories from the baseline using this button. Finally, there is an Add button, which allows you to add a new rule to the baseline. Going back to the Duplicate button, you can see how much of a time saver these two buttons can really be if used together.

Desired Configuration Management Reporting

After a short period of time you should be able to run several of the reports included with Configuration Manager for DCM. There are three categories included in the default list of reports: DCM assignment (2), compliance (17), and errors (6). These reports can be customized to suit your needs or you can build your own reports if they don't provide the level of detail you require.



IMPLEMENTING ENERGY STAR POWER MANAGEMENT CONFIGURATION PACK

Mr. George T. Management comes into your office and states that he wants to ensure all machines enter system standby or hibernate after 30 minutes of inactivity, have monitors enter sleep mode after 5 minutes of inactivity, and issue a warning notification if the screen savers are disabled. What is your plan of action?

- 1. First, download the Energy Star Power Management Configuration Pack from Microsoft's site: www.microsoft.com/downloads/details.aspx?FamilyId=C8324323-2159-4E49-988C-3505653EAA26&displaylang=en&displaylang=en
- 2. Run the MSI File to extract the files into a temporary directory.
- 3. Open the Configuration Manager Admin console and navigate to the Desired Configuration Management node located under Site Database, Computer Management.
- 4. Right-click on Configuration Items and choose to Import Configuration Data.
- Click Add to import the Energy Star Power Management Configuration cab (Installer file) file. Browse to the location where you extracted the downloaded file.
- **6.** Click Next after you have imported the configuration items and configuration baselines from the Configuration Pack.
- Click Next on the Summary dialog box. Click Close on the Completing the Import Configuration Data Wizard.

Now you will have two Guidelines and one Recommendation under the Configuration Items and one new Energy Star Baseline.

The Energy Star Configuration Pack is a DCM that uses ENERGY STAR defined efficiency levels and recommendations based upon the ENERGY STAR program. The Configuration Pack has the following levels and recommendations:

- ◆ Computers enter system standby or hibernate after 30-60 minutes of inactivity
- ◆ Computer monitors enter sleep mode after 5 to 20 minutes of inactivity
- Warning notifications if screen savers are disabled.

The Bottom Line

Enabling the DCM Agent Until the DCM agent is enabled for your Configuration Manager clients, your clients will not evaluate any of the configuration baselines. This is the first step in using DCM to validate client settings.

Master It Enable the DCM agent for the Configuration Manager clients.

Creating Configuration Items Configuration items are the pieces of the puzzle that make up the picture called a configuration baseline. There are a number of different configuration item types in Configuration Manager, and depending on the type you choose to create, you are presented with certain options when assembling your configuration item. The steps to create configuration items were covered in the first part of this chapter, which included several examples on how to create the different types of configuration items.

Master It Create a configuration item for an application that checks a registry string value.

Assemble Configuration Baseline This is where you take one or more of the CIs and put them together into a package that the Configuration Manager client downloads and at the scheduled time validates by checking the CIs against the computer. The Configuration Manager client then reports the outcome of those checks back to Configuration Manager where you can then run reports to see if your clients are within the specified configuration or not. These steps were covered in the last section of the chapter.

Master It Assemble a configuration baseline with one or more configuration items you have created.

Chapter 13

Mobile Device Management

With the ever-increasing number of mobile users, companies are looking at ways to inventory, collect data on, and manage their mobile devices. Configuration Manager 2007 mobile device management enables the administrator to discover and manage mobile devices, all from within one console.

Its options for mobile devices are much like those available for managing desktops and laptops; Configuration Manager 2007 can perform hardware inventory, software inventory, file collection, software distribution, and mobile device configuration on supported device.

In this chapter, you will learn how to do the following:

- ◆ Enable a mobile device management point
- Verify the health of mobile clients

Setting Up a Mobile Device Management Point

The steps to activating a management point to extend to mobile devices are quite simple. Earlier chapters showed you how to activate management points and other site system roles. However, in case you jumped right to this chapter, here is a detailed list of the steps required for setting up a management point role:

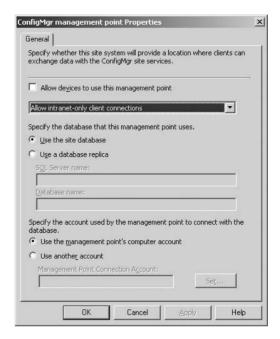
- 1. Open the Configuration Manager 2007 console, and expand the Site Management node.
- **2.** Expand the Site ➤ Site Settings ➤ Site Systems node.
- **3.** Select the management point server name.
- 4. Under Roles, right-click ConfigMgr Management Point, and choose Properties.
- 5. Check the box Allow Devices To Use This Management Point, as shown in Figure 13.1.
- Click OK.

It will take a few minutes for the management point to be configured for Windows Mobile devices, but you can monitor a few things to ensure that the installation has completed. First, you can check the DMPSetup.log file that resides in the Program Files\Microsoft Configuration Manager\Logs folder on the site server. You can also monitor the Rolese~1.exe file with Task Manager to check the installation process.

Once you have it set up correctly, the management point will provide data for Configuration Manager 2007 device management. The management point is the sole point of communication for the mobile device clients and Configuration Manager 2007. The mobile device management point provides policies to the mobile devices that manage the configuration and software installation

instructions. These instructions include hardware and software inventory, file collection, software installation, and configuration.

FIGURE 13.1
Configuring management point properties



Enabling Distribution Points for Supporting Mobile Devices

As we discussed in earlier chapters, distribution points are used to store the packages (containing, for example, software updates) that are distributed to clients on the Configuration Manager site. The mechanism is no different when it comes to distributing packages to mobile device clients. At least one distribution point is required if you are going to distribute packages to mobile devices.

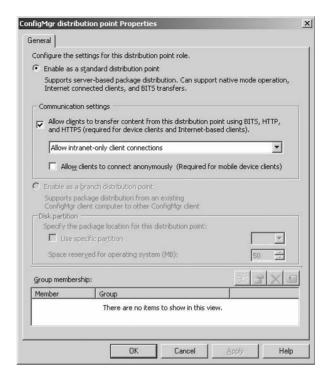
To enable a distribution point to support mobile devices, follow the steps listed here. Before you begin, make sure the Background Intelligent Transfer Service (BITS) is enabled on IIS.

- 1. Open the Configuration Manager 2007 console, and expand the Site Management node.
- **2.** Expand the Site ➤ Site Settings ➤ Site Systems node.
- 3. Select the distribution point server name.
- 4. Under Roles, right-click ConfigMgr Distribution point, and choose Properties.
- Check the box Allow Clients To Transfer Content From This Distribution Point Using BITS, HTTP, and HTTPS (Required For Device Clients And Internet-Based Clients).
- **6.** Check the box Allow Clients To Connect Anonymously (Required For Mobile Device Clients), shown in Figure 13.2.
- 7. Click OK.

Mobile device clients will receive policy and package information from the management point, just as normal clients do. Software is handed down to the mobile device through a distribution point. Windows Mobile device clients download content from distribution points using HTTP or

HTTPS. The distribution points need to be configured not only for HTTP and HTTPS traffic but also to allow all anonymous connections from the Windows Mobile device clients.

FIGURE 13.2
Configuring distribution point properties



Configuring the Mobile Device Client Agent

The Mobile Device Client Agent is used to configure what actions you want to take on each of the mobile devices. Just like the Configuration Manager client agent for managed computers, the Mobile Device Client Agent provides the ability to enable and configure the mobile device poll settings, software inventory, hardware inventory, software distribution, and file collection settings. These settings are for all the mobile devices within the Configuration Manager 2007 site hierarchy.

To enable or change the Mobile Device Client Agent properties, you will need to open the Configuration Manager administrator console:

- 1. Open the Configuration Manager 2007 console, and expand the Site Management node.
- **2.** Expand the Site ➤ Site Settings ➤ Client Agents node.
- 3. Right-click Mobile Device Client Agent, and choose Properties.
- **4.** On the Mobile Device Client Agent Properties dialog box's General tab, specify the Poll Interval, Retry Delay, and Number Of Retries settings, as shown in Figure 13.3.

The Poll Interval setting specifies how often the mobile device client will poll the management point for new policy. Valid settings range from 1 minute to 23 hours, with a default value of 30 minutes.

FIGURE 13.3 The General tab of the Mobile Device Client Agent Properties dialog box



The Retry Delay setting allows the administrator to customize the amount of time between retries when the mobile device fails to connect to the management point. Valid settings have the same range as the poll interval, 1 minute to 23 hours.

POLL INTERVAL AND RETRY SETTINGS

Note that the poll interval must be less than the retry delay multiplied by the number of retries.

The Number of Retries setting configures the number of times the client retries its connection to the management point; valid settings range from 0 to 99 retries.

- 5. On the Software Distribution tab, shown in Figure 13.4, enable the software distribution to device clients.
- **6.** The Software Inventory tab, shown in Figure 13.5, is used to enable and specify software inventory for the mobile devices.
 - To add files to be inventoried, click the New button, and add the information to be inventoried. You can use a wildcard character (*) to collect groups of files. These settings are the same as enabling file inventory on a regular Configuration Manager client.
- On the Hardware Inventory tab, shown in Figure 13.6, specify how often the hardware inventory should run.
- **8.** On the File Collection tab, shown in Figure 13.7, specify how often the file collection should run and what files are to be collected.

To add files to be collected, click the New button, and add the information defining what is to be collected. You can use a wildcard character (*) to collect groups of files. These settings are the same as for enabling file inventory on a regular Configuration Manager client.

FIGURE 13.4 The Software Distribution tab of the Mobile Device Client Agent Properties dialog box

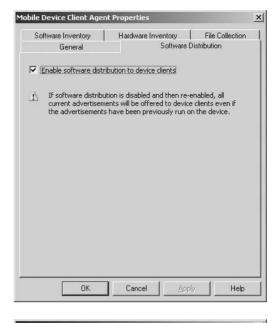
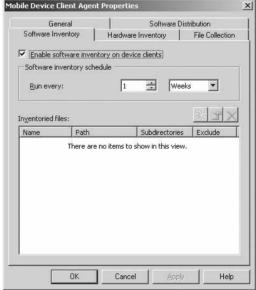


FIGURE 13.5
The Software Inventory tab of the Mobile
Device Client Agent
Properties dialog box



Extending Inventory on Client Desktop Computers

To discover desktop clients that have mobile devices syncing with them, the hardware inventory for these desktop clients needs to be extended. Microsoft provides the Device Management Inventory Extension as a predefined package definition, available by default when you enable mobile client support within Configuration Manager 2007. This package is required only for systems running Windows XP and older, because Vista has this capability already built in.

FIGURE 13.6

The Hardware Inventory tab of the Mobile Device Client Agent Properties dialog box

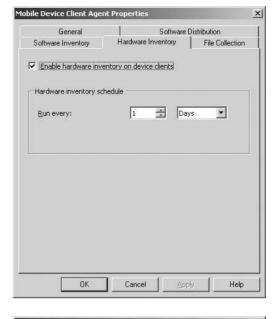


FIGURE 13.7

The File Collection tab of the Mobile Device Client Agent Properties dialog box



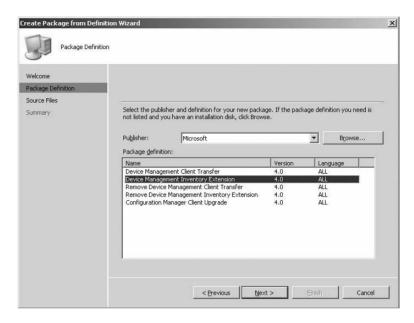
Setting Up the Device Management Inventory Extension Package

Take these steps to set up the Device Management Inventory Extension package:

- 1. Navigate to the Computer Management ➤ Software Distribution node of the Configuration Manager 2007 administrator console.
- 2. Right-click Packages, and choose New.

- 3. Select Package From Definition.
- 4. Click Next on the Welcome page.
- **5.** Select the Device Management Inventory Extension version 4.0 definition file, as shown in Figure 13.8, and click Next.

FIGURE 13.8
The Package Definition page of the Create
Package From Definition Wizard



- **6.** Choose Always Obtain Files From A Source Directory, and click Next.
- 7. Select Local Drive On Site Server, and use the following source directory, as shown in Figure 13.9: <installation directory>\DeviceClientDeployment\Inventory Extension.
- 8. Click Next and then Finish.

Specifying a Distribution Point for the Package

You will need to specify which distribution points you want to assign this package to in order for it to be available. Take the following steps:

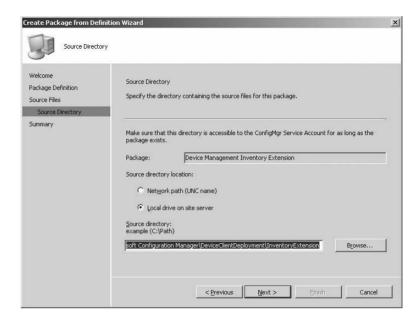
- Expand Packages, expand Microsoft Device Management Client Transfer, and select Distribution Points.
- 2. Right-click Distribution Point, and select New.
- **3.** Select your server, and click Next and finally Close.

Advertising the Package to Clients

Now this package can be advertised to clients:

1. Open the Configuration Manager 2007 console.

FIGURE 13.9
The Source Directory
page of the Create
Package From Definition Wizard



- 2. Expand the Site Database node.
- 3. Expand the Computer Management node.
- **4.** Expand the Software Distribution node.
- 5. Right-click Advertisements, select New, and then click Advertisement.
- 6. Fill in the information as desired, and then, under Packages, select Microsoft Device Management Inventory Extension. Then select the collection to install the Device Management Inventory Extension, and click Next.
- 7. Specify the schedule of when the program will be advertised to the members of the collection, and if desired, specify whether the assignment is mandatory. Click Next.
- 8. Choose the default settings in the Distribution Points dialog box; when the client is connected to a fast connection, it will download the content from the distribution point and run the program locally, and when the client is on a slow connection, it will not run the program. Click Next.
- **9.** The users do not need any interaction with this program, so in the Interaction dialog box leave both selections deselected. Click Next.
- **10.** Specify the security settings you desire for the advertisement, and click Next.
- **11.** On the Summary page, click Next.
- 12. Click Close.

Now that you have the advertisement for the Microsoft Device Management Inventory Extension created, it will install on all the devices within the collection.

You can verify that the Device Management Inventory Extension has been installed on the machines by looking at the Software Distribution home page summarization. To do so, expand the Site Database node, choose Computer Management, and finally click Software Distribution.

Now you are ready to connect your Windows Mobile device through ActiveSync. We'll show how to connect the mobile device through ActiveSync so that Configuration Manager will detect that a mobile device is connected through the ActiveSync connection. Once you have made this connection, open the Control Panel, and start Configuration Manager. Go to Configuration Manager Properties, click the Actions tab, and select Hardware Inventory Cycle. Once you have Hardware Inventory Cycle selected, click Initiate Action.

Note that the hardware inventory cycle can take a minute to process the hardware inventory data into the Configuration Manager site database.

Once the data has been processed and the site database has gathered all the hardware information from the client, the client computers with ActiveSync will appear in the following reports (Figure 13.10):

- Configuration Manager 2007 Desktops Reporting an ActiveSync-Connected Device Without a Configuration Manager 2007 Device Client
- Configuration Manager 2007 Desktops Reporting a Connected Windows Mobile Device

FIGURE 13.10
ActiveSync Service Status report

Report Name: Category: Comment: Parameters:	ActiveSync Se Device Manag Displays the stat		PCs running ActiveSync
11/28/2008 7:53:36	PM		(Number of Records: 1
11/28/2008 7:53:36 Sync PC Name	PM User Name	Major ActiveSync Version	(Number of Records: 1 Minor ActiveSync Version

For sites with SMS clients installed, there is also a built-in report that will display all the SMS client computers that have ActiveSync-connected devices that do not have the SMS device client installed, and its name is SMS Client Computers Reporting ActiveSync-Connected Devices Without SMS Device Client.

Installing the Client Software on a Mobile Device

Before you can start managing your mobile devices, you must get the client software installed on each mobile device. You basically have three ways to get the mobile client installed on a mobile device. You can install it manually, install it via connected computers, or install it over the air.

Editing the Device Client Deployment File

No matter which method you choose to install the mobile device client on devices, you must first manually edit the DMCommonInstaller.ini or ClientSettings.ini file to fit your environment. These files define the behavior of the mobile device client deployment process. They are located in the <Configuration Manager installation folder>\ DeviceClientDeployment\ClientTransfer folder.

The DMCommonInstaller.ini file is used when installing the mobile client using ActiveSync with a Configuration Manager 2007 client or when manually synchronizing with a desktop

computer. The ClientSettings.ini file is used when using over-the-air upgrade/install methods or when using a digital memory card or other method to install the client. The files each contain guidance on specific options that need to be changed.

For Configuration Manager 2007 to know what type of mobile client needs to be installed, you must manually set up a new folder to keep the files discussed earlier and ensure they are ready for your mobile clients. This folder will be transferred to and run on the mobile devices.

- 1. Create a new folder called C:\DeviceClient.
- 2. Copy the all the files into C:\DeviceClient from the following location: <Configuration Manager installation folder>\DeviceClientDeployment\ClientTransfer\
 <LanguageCode folder>.
- **3.** Copy the all the files into C:\DeviceClient from the following location: <Configuration Manager installation folder>\DeviceClientDeployment\ClientTransfer\.
- **4.** Open and edit the file C:\DeviceClient\dmcommonistaller.ini; this file contains various sections for each supported Windows Mobile and Pocket PC device. For the purpose of this book, we will be concentrating on the Windows Mobile 6 device. Search the DMCommonInstaller.ini file for the "Windows Mobile 6.0 Pocket PC" section.
- 5. Once you locate that section, you will see this line:

DMServerName=myDmpServer

Edit that line by changing myDMPServer to your local device management point computer name.

By default, the DMCommonInstaller.ini file is set up to install the device client. If necessary, you can configure its installation option by changing the ClientInstallAction line as follows:

```
; Client Install Action:
; Set to 'None' to perform no change in DM client state
; Set to 'Install' to install the DM client
; Set to 'Uninstall' to remove the DM client
ClientInstallAction=Install
```

7. However, you want the client to install, so you will not change this area. Since within this book you are not deploying certificates, you will need to change the CertEnrollAction=Enroll line to CertEnrollAction=None.

Deploying the Device Client Installer to Clients

Now that you have copied the files and edited the DMCommonInstaller.ini file, you are ready to deploy the Device Client Installer to your Configuration Manager clients. This will then cause the Device Client Agent to be installed on the Windows Mobile devices when they are connected through ActiveSync.

CREATING A DEPLOYMENT PACKAGE

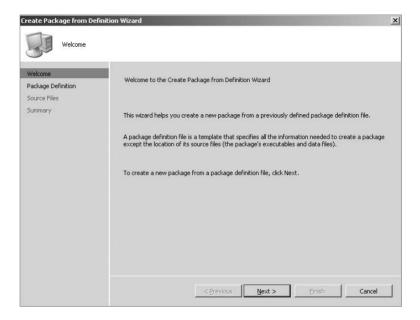
First you must create a package that contains the software you want to install on the mobile devices:

1. Within the Configuration Manager console, expand Site Database, then Computer Management, and finally Software Distribution.

Right-click the Software Distribution node, select New, and then click Package From Definition.

This opens the Create Package From Definition Wizard welcome page, shown in Figure 13.11.

FIGURE 13.11 Create Package From Definition Wizard's Welcome page



- **3.** Click Next on the Welcome page. You will now be presented with the Create Package From Definition Wizard's Package Definition dialog box, shown in Figure 13.12. Select Device Management Client Transfer, and then click Next.
- **4.** On the Create Package From Definition Wizard's Source Files page, select Always Obtain Files From A Source Directory, shown in Figure 13.13, and click Next.
- **5.** Now you are presented with the Create Package From Definition Wizard's Source Directory page. Select local drive on site server, and browse to the directory C:\DeviceClient, shown in Figure 13.14.
- **6.** Click Next, and you will be able to click Finish on the Create Package From Definition Wizard's Summary page, shown in Figure 13.15.

SPECIFYING DISTRIBUTION POINTS AND ADVERTISING THE PACKAGE

Now you will need to specify your distribution points for this package:

- Expand Packages, expand Microsoft Device Management Client Transfer, and select Distribution Points.
- 2. Right-click Distribution Point, and select New.
- **3.** Select your server, and click Next and finally Close.

FIGURE 13.12 Create Package From Definition Wizard's Package Definition page

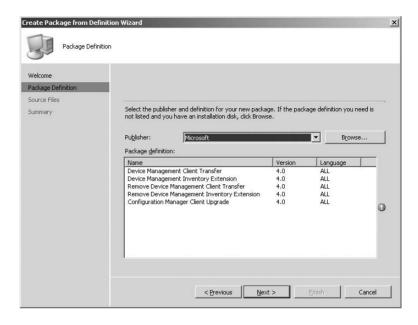
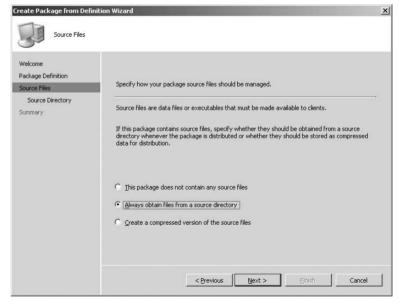


FIGURE 13.13
Create Package From
Definition Wizard's
Source Files page



After you have your package created, you will need to create an advertisement in order to distribute the package:

- 1. Browse to and expand Advertisements, and select New.
- **2.** On the New Advertisement Wizard's General page, fill in the name, and select your package and the collection you want to advertise the package to, as shown in Figure 13.16.

FIGURE 13.14
Create Package From
Definition Wizard's
Source Directory page

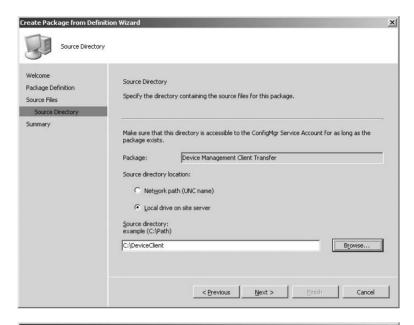
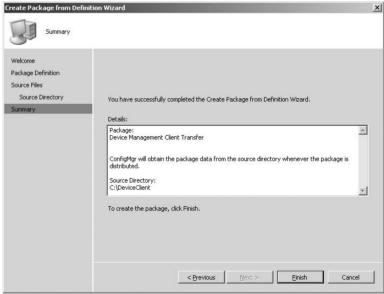


FIGURE 13.15 Create Package From Definition Wizard's Summary page



- **3.** Now you will be presented with the New Advertisement Wizard's Schedule page, shown in Figure 13.17. Click Next.
- **4.** In the New Advertisement Wizard Distribution Points dialog box, shown in Figure 13.18, keep the defaults, and click Next.
- **5.** Then, on the New Advertisement Wizard's Interaction page, shown in Figure 13.19, keep the defaults, and click Next.

FIGURE 13.16 New Advertisement Wizard's General page

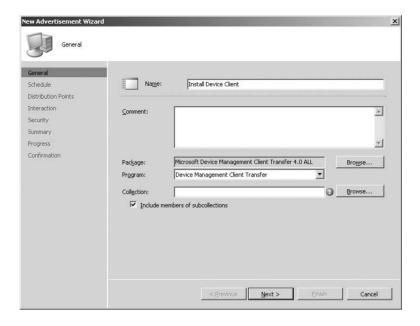
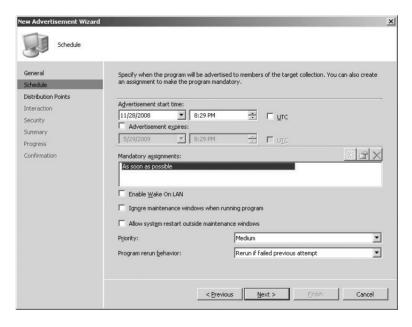


FIGURE 13.17 New Advertisement Wizard's Schedule page



6. On the New Advertisement Wizard's Security page, set your security as you need, and click Next. Now you will be presented with the New Advertisement Wizard's Summary screen. Click Next, and finally click Close.

FIGURE 13.18
New Advertisement
Wizard's Distribution Points page

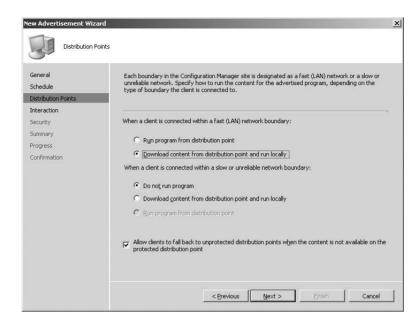
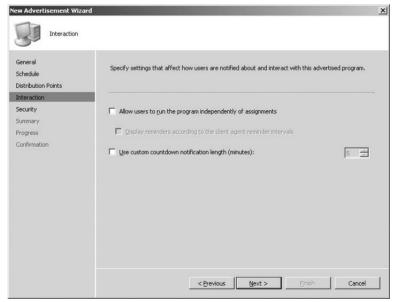


FIGURE 13.19
New Advertisement Wizard's Interaction page



Verifying Client Installation on Mobile Devices

You can verify the installation of the mobile device client in a few ways, depending on the administrator's preference. You can verify the clients by reviewing collection membership, by reviewing the mobile device client installation logs, by using the mobile device itself, or by using reports.

Verifying Using Collection Membership

To verify using collection membership, follow these steps:

- 1. Navigate to the System Center Configuration Manager console, and click Site Database.
- 2. Click the Computer Management node.
- **3.** Click the Collections node.
- 4. Select the All Windows Mobile Devices collection.
- **5.** Review the results pain to verify the client is in the collection.

Verifying Using Log Files

You can also use the log files to verify that the mobile device client was installed. Just as with other Configuration Manger 2007 clients, installation logs are created on the mobile device during the installation of the mobile client. There are three log files created on the device: DMINstaller <date stamp><time stamp>.log, DMClientSetup<date stamp>.log, and DMSvc<date stamp><time stamp>.log.



Real World Scenario

"WE NEED TO KNOW ALL THE WINDOWS MOBILE 6.X DEVICES."

George T. Management sends a request to your boss asking for the number of Windows Mobile 6.x devices being managed within the organization.

After getting this request, you consider just making a report to view, but you think a bit longer and wonder why Mr. Management needs this request. After some investigating, you find out Mr. Management will need to install an application on every Windows Mobile 6.x device. So, you decide it's best to create a collection to handle this task:

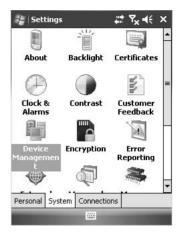
- 1. Open the Configuration Manager 2007 administrator console.
- 2. Navigate to the Site Database node.
- 3. Expand Computer Management.
- 4. Expand Reporting.
- 5. Right-click Report, and choose New Report.
- **6.** Name the report All Windows Mobile 6.x Devices, and specify a category of Windows Mobile Devices.
- 7. Add the following query to the Query rule by clicking Edit SQL Statement:

```
SELECT SELECT v_R_System.ResourceID, v_R_System.ResourceType, v_R_SYSTEM.Name0, v_R_System.Client0
FROM v_R_System where Operating_System_Name_and0 like 'Windows CE 5.2%'
```

Verifying Installation on the Mobile Device

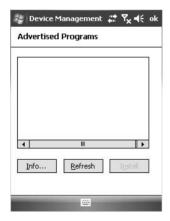
To verify the device installation on the Windows Mobile device, click Start on the device, and then click Settings. On the Settings tab, you will see Device Management icon, shown in Figure 13.20.

FIGURE 13.20
The Device Management icon on the mobile client



Clicking the Device Management icon reveals the Advertised Programs window, as shown in Figure 13.21, displaying any advertised programs that are available to the client.

FIGURE 13.21
The Advertised Programs window



Selecting the Info button on this screen will display the connection information that was configured for your site, shown in Figure 13.22.

Using Reports to Verify Installation

You can use a good number of reports to verify the installation status as well. Plus, with any report, you can build your own if you need some additional information.

FIGURE 13.22
Device Management info tab



Microsoft includes the following reports with Configuration Manager 2007 to help you with mobile clients:

- ◆ All Device Clients
- Device Client Agent Deployment Failure Report
- Device Client Agent Deployment Status Details
- ◆ Device Client Agent Deployment Success Report
- Device Client Agent Health Summary
- Device Client Information
- Device Client in Healthy Condition
- Device Client in Unhealthy Condition Due to Certificate Issues
- Device Client in Unhealthy Condition Due to Communication Issues
- ◆ Device Client in Unhealthy Condition Due to Local Client Issues
- SMS Client Computers Reporting ActiveSync-Connected Devices Without SMS Device Client
- ◆ SMS Client Computers Reporting an ActiveSync-Connected SMS Device Client

All of these reports are grouped under the category of Device Management under the Reports node.

Deploying Software to Mobile Clients

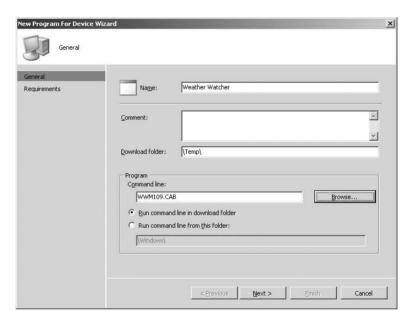
Configuration Manager 2007 allows administrators to deploy software to the mobile device client individually or in groups. The steps for deploying software to mobile clients are basically the same as we discussed in earlier chapters for deploying software to any Configuration Manager client.

Deploying software to mobile clients requires the following steps:

- 1. Create a package.
- 2. Create the program.
- 3. Select the distribution points.
- 4. Advertise the package.

One difference is that when creating the program for a device, you will be selecting Program For Device when you create the program; Figure 13.23 shows deploying Weather Watcher to the mobile devices.

FIGURE 13.23New Program For Device Wizard's General page



Then follow these steps:

- Once you create your new program for the device and click Next, you will be presented
 with New Program For Device Wizard's Requirements page, as shown in Figure 13.24.
 You can change the requirements for the device in order for the program to install onto the
 device. Click Finish.
- 2. Set your distribution point.
- **3.** Just as when creating packages for regular clients, you need to create an advertisement for your mobile client. As you can see in Figure 13.25, it looks very similar to what you saw when deploying advertisements to regular clients.
- **4.** All the other settings are very similar, so fill in the information appropriately, and click Next. The next page looks somewhat different from what you've seen with regular advertisements, as shown in Figure 13.26.

FIGURE 13.24 New Program For Device Wizard's Requirements page

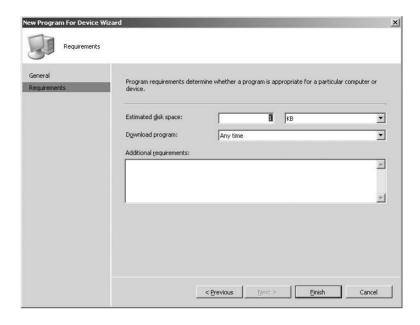
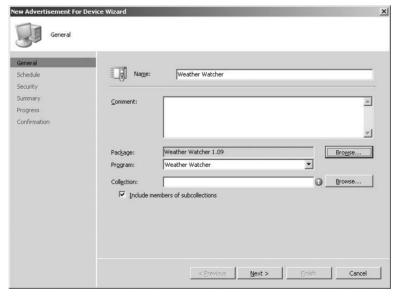
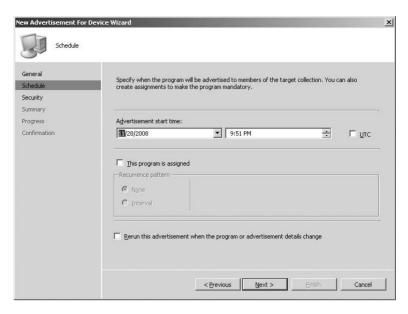


FIGURE 13.25 New Advertisement For Device Wizard's General page



- **5.** Click Next, and you will be presented with the Security Wizard; make the necessary changes for your environment, and then click Next. On the Summary page, click Next and then Close to complete the creation of the advertisement.
- **6.** Now that the package and advertisement have been created and advertised to the collection, you can force the Windows Mobile device to retrieve policies so the programs will install to the device.

FIGURE 13.26 New Advertisement For Device Wizard's Schedule page



- 7. On the Windows Mobile device, select Start, and then click Settings. On the Settings menu, click the System tab. From this menu, you can select the Device Management icon. Depending on the timing, your advertised program might not appear yet, but clicking Refresh will force the Windows Mobile device to retrieve any policy from the device management point.
- **8.** Once you see the program listed, select it, and then click Install. This will copy the program locally to the device and then install it to the client, as shown in Figure 13.27.

FIGURE 13.27
Advertised Programs
window on the mobile
device



Using Reports to Verify Mobile Client Health

To verify your mobile clients are able to receive policy and report inventory, you can use some health checks. The following reports are available to ensure your mobile clients are staying configured properly:

- Device Client Agent Deployment Failure Report
- Device Client Agent Deployment Status Details
- Device Client Agent Deployment Success Report
- Device Client Agent Health Summary
- Device Client in Healthy Condition
- Device Client in Unhealthy Condition Due to Certificate Issues
- Device Client in Unhealthy Condition Due to Communication Issues
- Device Client in Unhealthy Condition Due to Local Client Issues

The Bottom Line

Enable a mobile device management point. Setting up a mobile device management point within Configuration Manager gives administrators the ability to manage mobile devices within the Configuration Manager 2007 site.

Master It How do you enable a mobile device management point?

Verify the health of mobile clients. Configuration Manager 2007 has some prebuilt reports to help verify the health of mobile device clients.

Master It View the health status of mobile devices using reports.

Chapter 14

Network Access Protection

This chapter presents the basics of what network access protection (NAP) is and how you can use it with Configuration Manager 2007 to help maintain a healthy and secure network. NAP is a new technology introduced by Microsoft with the release of Windows Server 2008 and is built into both the server and client operating systems.

In this chapter, you will learn how to do the following:

- Identify the components that make up NAP and their roles
- Integrate your choice of the NAP enforcement methods with your current Configuration Manager 2007 deployment
- Deploy NAP with Configuration Manager 2007 in a phased approach to minimize your risk

Introducing Network Access Protection (NAP)

NAP is a set of technologies introduced with the release of Windows Server 2008 on the server and in Windows XP Service Pack 3 and Windows Vista on the client. These technologies have been built into the operating systems of these platforms, and you can manage them via Group Policy in a Windows environment.

There exists today a market for products and solutions based on a common industry concept called *network access control* (NAC). Microsoft's NAP is its entry into this market, so be aware that the terms NAP and NAC mean very different things. One is very specific to Microsoft, and the other is more an industry-wide term.

The NAP technologies allow administrators to create network access policies for machines that are connecting to the network. In these policies, administrators can define requirements that machines connecting to the network must meet. For example, a policy could require that a machine has a firewall installed and running, that it have an antivirus program installed and running, or that the machine be up-to-date with patches.

Policies can also define what actions should be taken for machines that meet the defined requirements or, more importantly, for the machines that do not meet the defined requirements. A third-policy option should also be put in place for machines that are not capable of running NAP. Most commonly these are older machines that are not running the latest operating system or service pack from Microsoft. Today, these machines would be those running a service pack older than Windows XP Service Pack 3.

Since NAP is designed to evaluate computers as they are coming onto the network or after they are already on the network, the technology was built to support a variety of what are called enforcement methods. The enforcement methods most commonly used with Configuration Manager are as follows:

- ◆ Dynamic Host Control Protocol (DHCP)
- 802.1x (wired or wireless)
- ◆ IPsec authentication (Internet Protocol security)
- ◆ Virtual private network (VPN) access

A fifth method, Terminal Server Gateway (TSG), is also available. However, because a TSG deployment is specific to a Microsoft product offering and probably not a way that clients would commonly connect to a network, we will not cover this enforcement method with regard to SCCM 2007 integration.

We will discuss best practices for integrating Configuration Manager 2007 with each of the common enforcement methods, because each has unique requirements for network design and server availability. It is important to understand how each enforcement method handles the scenario in which a machine does not meet the defined policy requirements and is required to be quarantined.

NAP supports the concept of quarantining noncompliant computers if they do not meet the defined requirements, but more important, it also supports the concept of autoremediation of these machines without the user having to interact with the machine. This is an important feature since it can have big help desk savings for organizations that want to deploy NAP with the autoremediation feature enabled.

We will briefly go over each enforcement scenario and how NAP can quarantine machines that do not meet the defined network policy later in this chapter.

Requirements for Implementing NAP on Your Network

As mentioned, the components required to implement NAP have been built into the operating system and have shipped either with the operating system or in a service pack.

To deploy NAP on your network, you will need a NAP-capable desktop operating system (Windows XP Service Pack 3 or later) and at least one member server running Windows Server 2008 with the network policy server (NPS) role installed. The NPS role is an optional role that you install and configure via the Role Management Tool (RMT) and via the NPS Microsoft Management Console (MMC) snap-in.

An additional requirement if you are integrating Configuration Manager 2007 and NAP is that you will have to extend your Active Directory schema for Configuration Manager, as discussed in Chapter 2. Note that the requirement for Windows Server 2008 is simply to have at least one member server. What this means is that your Windows Server 2008 member server can reside in an Active Directory forest that is not Windows Server 2008 based. Thus, you can easily insert NAP into your network without having to do a major Active Directory upgrade of any kind.

Once you have all the pieces in place and your policies configured on your Windows Server 2008 NPS, you will then need to enable the NAP agent service on the clients that you want to participate in NAP. You can do this via Group Policy, via a logon script, or manually if you like.

The second step on the client is to then enable the proper quarantine enforcement client (QEC) on your desktops. You can do this via Group Policy, via a logon script, or manually. You will see that there is a QEC for each supported enforcement method. For example, if you are deploying

DHCP-based NAP, you would need only to enable the DHCP QEC and the NAP agent service on your clients for those machines to participate in NAP.

A Quick Look at the NAP Architecture in the Operating System

As previously mentioned, the core components required for NAP are built into the operating system and can be managed via Group Policy or a script. This allows the administrator to enable and start the NAP agent service and to configure the individual QECs.

Higher up in the architecture sit several other key components, which are part of the NAP ecosystem. It is important to understand their roles and how they operate. The following are explanations of these components:

The NAP statement of health (SoH) The NAP SoH is the single most important piece in a NAP deployment simply because it contains the health, or *posture*, information for the machine that is attempting to connect to the network. This data is in a binary format and is transmitted to the NPS by a variety of means, each of which is unique to the enforcement method that you have deployed.

The SoH is also important to understand because it has been accepted as an industry standard. It is recognized by the Trusted Computing Group (TCG), a standards body that oversees developments in the NAC market. Microsoft took the SoH format and protocols to the TCG in the spring of 2007 for standards acceptance and was granted it. What this means for you as a customer is that if you deploy components from vendors that are part of the TCG, you are assured interoperability with the NAP platform. This is an important point to note since many vendors in the NAC market are selling proprietary solutions that are not based on any kind of standard.

System health agents (SHAs) An SHA is a component installed on the client machine that is configured to do NAP. Windows ships with an SHA as part of the operating system; it is called the Windows System Health Agent (WSHA).

An SHA is responsible for reporting its status to the NAP agent service at network connection time so that the NAP agent service can create an SoH to send to NPS for evaluation.

SHAs can monitor just about anything on the client machine imaginable. System Center Configuration Manager 2007 has its own SHA, which monitors the patch state of the machine. We will go into more detail on the Configuration Manager SHA later in this chapter.

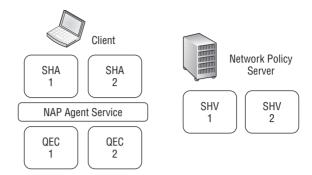
Also note that Microsoft has produced an SHA software development kit (SDK) for anyone to use who wants to write their own custom SHA.

System health validator (SHV) An SHV corresponds directly with the SHA that resides on the client machine. The biggest difference is that an SHV is installed as a plug-in to the NPS on your network and is responsible for evaluating the SoH information that is sent by the SHA via the NAP agent service.

Administrators will install the Configuration Manager 2007 SHA on all their desktop machines as well as the Configuration Manager 2007 SHV on their NPS servers. The SHV usually has a customer interface that is exposed in NPS so that administrators can create customer network access policies for client machines coming onto the network.

We will discuss the Configuration Manager 2007 SHV in more detail later in this chapter. Figure 14.1 illustrates the SHA/SHV model.

FIGURE 14.1
The NAP SHA/SHV model



Exploring the NAP Enforcement Methods

How does each of the commonly used NAP enforcement methods quarantine a noncompliant computer? When you are evaluating a NAP deployment, this is the most important aspect to consider since it may require some network redesign or possibly the introduction of network authentication technologies that you may not have in place today.

802.1x NAP (Wired or Wireless)

The 802.1x network authentication standard has been around since the mid-1990s and was defined to be used primarily in wireless networks as a means of port access control. 802.1x also allows secure Remote Authentication Dial In User Service (RADIUS) authentication between the client machine and a back-end RADIUS server.

To do 802.1x NAP, you need the following components on your network:

- A client machine with an 802.1x supplicant (most newer operating systems have them built in, but third-party options are also available)
- ◆ An 802.1x-capable switch or wireless access point (WAP)
- A RADIUS server that is reachable by switches or WAPs on your network

Note that in the NAP world, an "802.1x-capable switch or access point" is defined as having one or both of the following characteristics:

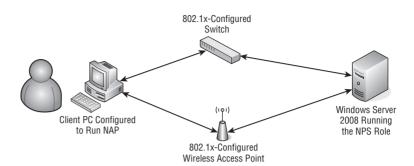
- It must support the capability to dynamically move machines from one virtual local area network (VLAN) to another.
- It must support the ability to dynamically apply port access control lists (ACLs) that are sent from the RADIUS server to the switch of WAP.
- ◆ The ACLs are used to control the client's access to the network.

Figure 14.2 illustrates how a machine connects to a network that has 802.1x NAP enforcement deployed.

Here's the process:

- 1. The client computer boots or connects to the network via a wired or wireless connection.
- The switch or WAP requests that the machine send its identity and credentials for authentication.

FIGURE 14.2 Connecting to a network via 802.1x NAP



- **3.** The client machine sends its identity and credential via a secure connection it has made with the NPS.
- **4.** As part of this process, the client also sends its SoH to the NPS.
- **5.** The NPS authenticates the machine or user and evaluates the SoH it has received against the current policies that the administrator has configured on NPS.
- **6.** Based on the results of the policy evaluation, information is sent to the switch or WAP that will tell it what kind of access the machine should receive.
- 7. To quarantine noncompliant machines in 802.1x NAP, either the NPS sends back VLAN tags to the WAP to tell the device which VLAN to put the machine in or it sends a set of ACLs to the device, defining the limitations of that machine's network access. These ACLs are usually an IP address, protocol, and port that the noncompliant machines can access.

DHCP NAP

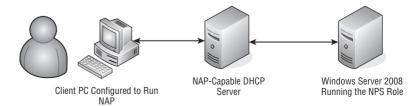
DHCP-based NAP is the simplest of the enforcement methods to deploy primarily because it has the fewest requirements from a server perspective. DHCP NAP is also the only enforcement method that doesn't have any kind of authentication or encryption options available, which makes it the least secure of the enforcement methods.

For DHCP NAP, you will need a NAP-capable DHCP server. At press time, the only NAP-capable DHCP server in the market was the Microsoft DHCP server built into Windows Server 2008. Just like the other enforcement methods, DHCP also requires a Windows Server 2008 member server running the NPS role.

On the client, you will also need the NAP agent enabled as well as the DHCP QEC. Because the server requirements are so simple for DHCP NAP, it is a common practice to run both the DHCP and NPS roles on the same physical or virtual machine.

Figure 14.3 illustrates how a client computer connects to a network that has DHCP NAP enforcement deployed.

FIGURE 14.3
Connecting to a network via DHCP NAP



Here's the process:

- 1. The client computer boots up or connects to the network and requests an IP address.
- During the negotiation with the DHCP server, the client machine sends its SoH to the DHCP server.
- 3. The DHCP server hands the SoH off to NPS for evaluation.
- **4.** Once NPS evaluates the SoH, the client will receive an IP address and, if necessary, will be quarantined on that network by having its route table modified so that it can communicate only with the remediation servers defined by the administrator.

Quarantine in DHCP NAP is handled by issuing the client a routable IP address for the network (so that it can connect to a remediation server), but no default gateway will be issued to noncompliant machines. In addition, the NAP service will modify the machine's route table so that it can connect only to the remediation servers that the administrator has defined in their NPS policy.

VPN NAP

For companies that have remote users who frequently use a VPN to connect to the corporate network, a solution like NAP is vital to keeping the network healthy.

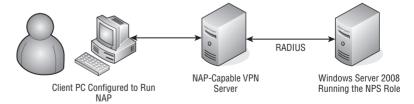
VPN NAP works in a similar manner to 802.1x NAP in that users will connect from a client machine to a VPN server and do a secure authentication to the NPS, which sits on the network behind the VPN servers.

The biggest difference between the VPN and 802.1x enforcement methods is how the quarantine is done. In VPN NAP, users are quarantined by having the NPS send back a set of IP filters to the VPN server that are then applied to that machine's connection to essentially quarantine that machine or limit its access on the network during that VPN session.

Like the previous enforcement methods, VPN NAP also requires a Windows Server 2008 member server, but for VPN you must also have a NAP-capable VPN server if you want to do "native VPN NAP." What this means is that to have the VPN server be the control point for that machine's network connection, it must support certain type length and values (TLVs) that the NPS will send to it. At press time, the only native NAP-capable VPN server on the market is the Routing and Remote Access Server (RRAS) role that ships as part of Windows Server 2008.

Figure 14.4 illustrates how a machine connects to a network that has VPN NAP enforcement deployed.

FIGURE 14.4 Connecting to a Network via VPN NAP



Here's the process:

- **1.** The user establishes a secure connection with the VPN server.
- **2.** During the authentication phase with the NPS, the client sends its SoH.

- 3. NPS evaluates the SoH and, based on the results of that evaluation, sends a set of IP filters to the VPN server if the machine fails the health policy evaluation and is deemed to be noncompliant.
- 4. Quarantine in VPN NAP is done by NPS sending a set of IP filters down to the VPN server to be applied to that machine's connection. By default, the IP addresses of the remediation servers that the administrator has defined in their NPS policy are what get applied as filters to the machine's connection if the machine matches a noncompliant policy when evaluated by NPS. Additional IP filters can also be added in the NPS interface to be sent to noncompliant machines.

IPsec NAP

IPsec NAP is the one enforcement method that is truly unique to Microsoft's NAP offering. Many competing NAC solutions offer support for 802.1x, DHCP, or sometimes both, but Microsoft's NAP is the only one that offers out-of-the-box support for IPsec.

IPsec is an authentication technology that packages several different protocols and allows administrators to create policies that will force every single connection on the network to be authenticated by the machine that is being connected to. Many people call IPsec a *peer-to-peer* authentication mechanism, which is a pretty accurate description of the technology and what it can do.

What is also unique about IPsec NAP is that it is the only enforcement method that supports the ability to encrypt data. This is a very attractive option for administrators who are looking to tighten the security of their network beyond doing security at layer 2 (with something like 802.1x).

IPsec NAP also introduces the requirement of an additional role to be deployed on the network, which is also unique to Windows Server 2008. This role is the health registration authority (HRA). The HRA's role is to issue health certificates to machines that pass the administrator-defined compliance policy for their network. In essence, the HRA acts as a subordinate certificate authority that chains up to a root certificate authority that exists on the network.

Figure 14.5 illustrates how a machine connects to a network that has IPsec NAP enforcement deployed.

Here's the process:

- 1. The client computer attempts to make a connection to a machine on the network (illustrated as a dotted line in Figure 14.5).
- **2.** The connection is refused if the machine does not have a health certificate, and the machine is told to contact the HRA to request a health certificate.
- **3.** The machine contacts the HRA, requests a health certificate, and, as part of that request, sends its SoH.
- **4.** The HRA sends the SoH to the NPS for evaluation, and if the machine is deemed to be compliant, a certificate is issued from the HRA to the machine.
- **5.** Quarantine in IPsec NAP is done by the NAP service by immediately deleting the health certificate that was issued to it by the HRA and by tearing down all active security associations that the machine has with other machines on the network.

via IPsec NAP Certificate Authority Health Registration Windows Server 2008 Client PC Configured to Run Authority (HRA) Running the NPS Role NAP

FIGURE 14.5 Connecting to a network

Preparing for NAP and Configuration Manager 2007 Integration

Now that you understand what NAP can do for you and what the deployment requirements are, we'll walk you through some of the steps you will need to take to integrate NAP into your current Configuration Manager 2007 infrastructure, and we'll cover how each enforcement method can affect the behavior of the Configuration Manager clients that will be requesting patches from your Configuration Manager servers.

File Server Secured by **IPsec Policy**

We will also discuss the three recommended phases of a NAP deployment in a Configuration Manager environment and the value of each phase. The ability to quarantine a machine that does not meet the requirements of your network is a very powerful tool to have at your disposal, but it also requires some additional thinking and can affect how the clients on your network access resources. The classic question to ask yourself when evaluating a solution like NAP is this: "Would you kick the CEO off the network if their machine was deemed to be noncompliant?" Everyone answers this question differently, but it is an important one to ask yourself because it can also apply to the hundreds or thousands of other machines on your network. If your organization requires network access to function properly, understanding the effects of NAP and Configuration Manager integration is critical.

Configuring Configuration Manager and NAP

The first assumption to be made here is that you have a working Configuration Manager 2007 infrastructure that is capable of distributing patches to the client machines that you manage.

The second assumption is that your client machines are all running a NAP-capable build (Windows XP Service Pack 3 or later) and that you have at least one member server running Windows Server 2008 with the NPS role installed. Also, we assume you have configured your client machines for NAP by enabling the proper QEC as well as the NAP agent service on those machines that you want to participate in NAP.

Once you have the infrastructure in place to do NAP, you will need to enable NAP on your Configuration Manager 2007 clients as well as install the SHV on your NPS server.

ENABLING YOUR CONFIGURATION MANAGER CLIENTS FOR NAP

To enable your Configuration Manager clients for NAP, follow these steps:

- In the Configuration Manager console, navigate to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ site code ➤ site name ➤ Site Settings ➤ Client Agents.
- 2. Right-click Network Access Protection Client Agent, and then click Properties.
- **3.** On the General tab, select the option Enable Network Protection On Clients.
- 4. Click OK.

Next, you will need to install the Configuration Manager 2007 SHV on your NPS. Take the following steps to install a system health validator point on a new site system server:

- In the Configuration Manager console, navigate to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ site code ➤ site name ➤ Site Settings.
- Right-click Site Systems, click New, and then click Server to launch the New Site System Server Wizard.
- On the General page, specify the server name, and if you cannot use the site server computer account for installation, specify an installation account. Then click Next.
- **4.** On the System Role Selection page, select System Health Validator.
- **5.** Click Next, click Finish, and then click Close.

INSTALLING A SYSTEM HEALTH VALIDATOR POINT ON AN EXISTING SITE SYSTEM SERVER

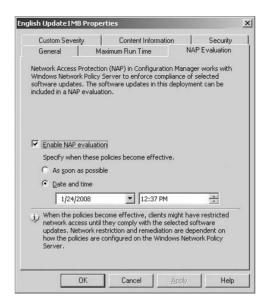
Take the following steps to install a system health validator point on an existing system server:

- In the Configuration Manager console, navigate to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ site code ➤ site name ➤ Site Settings.
- **2.** Right-click the existing site system server to which you want to add the system health validator point, and then click New Roles to launch the New Site Roles Wizard.
- **3.** On the General page, click Next.
- **4.** On the System Role Selection page, select System Health Validator.
- 5. Click Next, click Finish, and then click Close.

CONFIGURING CONFIGURATION MANAGER UPDATES FOR NAP

Now that you have enabled the proper components on the clients for both Configuration Manager 2007 and NAP, the next step is to configure Configuration Manager to enforce a particular set of updates to be enforced by NAP. Figure 14.6 shows an example.

FIGURE 14.6 Configuration UI for configuring NAP policy to specific patches



Here are the steps:

- In the Configuration Manager console, navigate to System Center Configuration
 Manager ➤ Site Database ➤ Computer Management ➤ Software Updates ➤ Update
 Repository.
- Select the software updates you want to deploy, right-click, and select Deploy Software Updates to launch the Deploy Software Update Wizard. (For more information about software updates, see Chapter 7.)
- Select the options you want to create for your software update deployment, and click Next until you come to the Set NAP Evaluation page.
- **4.** Click Enable NAP Evaluation, and then configure the effective date either by selecting As Soon As Possible or by selecting Date And Time and specifying the date and time that the policy will become effective.
- **5.** Click Next, Finish, and Close to complete the wizard.

The next step is to create NAP policies that will be evaluated as clients attempt to connect to the network. One of the great features of NPS in Windows Server 2008 is the NAP Wizard, which allows you to quickly create network access policies to start the first phase of your NAP deployment.

To get to the NAP Wizard in NPS, do the following:

- Launch the NPS snap-in either from an MMC console or via Start ➤ Administrator Tools ➤ Network Policy Server.
- 2. Click the main node titled NPS on the left.
- In the right pane, you will see a link to configure NAP; click that link to launch the NAP Wizard.

The first question you are asked in the NAP Wizard is what kind of network connection method you are configuring. This refers to the enforcement methods we have discussed in this chapter, and when you click the drop-down box, you'll see the options that we discussed earlier. We will discuss each of the enforcement methods and their impact on your Configuration Manager deployment when machines are deemed to be noncompliant and are put into a quarantine state.

Depending on which option you select, you will be taken down a different path by the wizard and asked to answer a few basic questions.

Once you complete the wizard, if you navigate to the Network Policy node in the NPS user interface, you will see that the wizard has created three policies for you: one policy for compliant machines, one for noncompliant machines, and one for machines that are not NAP-capable.

By default, machines that match the "compliant" policy are given full network access, and those that are "non-NAP capable" are denied network access. Of course, you can go into the NPS interface and change these defaults, but for the sake of this discussion, we are going to assume the defaults remain.

Phasing NAP into a Configuration Manager 2007 Environment

Most of Microsoft's deployment white papers and documentation refer to three phases of a NAP deployment. These are (in Microsoft's terms) *reporting mode, deferred enforcement*, and *full enforcement*.

Considering that NAP gives administrators the ability to quarantine machines from their network, NAP is not something you would simply "flip the switch on" for. With Configuration Manager 2007 and the ability to enforce NAP on a patch-by-patch basis, deploying NAP in these three phases is something very valuable. Let's look at each of these phases and how it relates to Configuration Manager:

Reporting mode This is the first recommended phase of a NAP deployment, and it allows administrators to start looking at the posture of machines on their network. Configuration Manager 2007 offers similar types of functionality with its Desired Configuration Manager feature, but in this specific case by turning on the NAP service for a select set of client machines (or on all clients if you want), this will tell the Configuration Manager SHA to send an SoH to the NPS at network connect time. In reporting mode, you will set your NPS policies to allow full network access for all machines. In Figure 14.7, you will see it is the top radio button that you would select for reporting mode.

Because you are not doing any kind of enforcement, what you are doing in reporting mode is gathering posture information and logging it. (NPS logs to the security event log of the server, or you can configure it to log to a SQL database.) Every time a machine connects and an SoH is received, your policy will allow that machine full access, and NPS will log information on the posture of that machine. This is a great way to see what machines on your network are up-to-date with the patches that you require and, more important, which machines are not up-to-date with patches.

Deferred enforcement The second phase of a NAP deployment is actually where your users will be introduced to NAP if their machines ever become noncompliant. In other words, if one of the machines that you have NAP enabled on ever becomes noncompliant or is missing a patch that you require, the user will see a dialog box on the desktop from NAP. The dialog box will look something like Figure 14.8.

FIGURE 14.7Policy configuration for NAP reporting mode

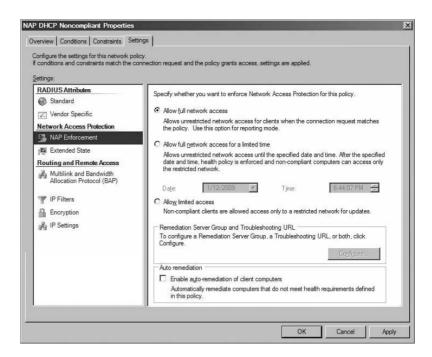
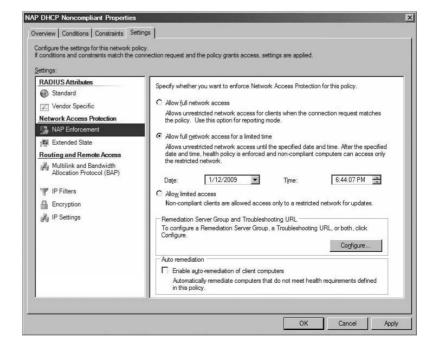


FIGURE 14.8
Policy configuration
for NAP deferred
enforcement



You will note that the dialog box includes a date and time defined by the administrator. In deferred enforcement, you are essentially warning your users that their machines are noncompliant, but you are still not restricting these machines from network access. If the user clicks this dialog box, they will be taken to another screen that includes instructions on exactly what actions they need to take to become compliant with your patch policy.

On the server side, to set this up you would select the second radio button in your network policy, which will then allow you to enter the date and time that you are allowing users on your network until they will be put into a quarantine state.

Deferred enforcement is a very powerful option for a couple of reasons:

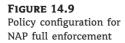
- It allows your users to police themselves and keep their machines compliant without having to be quarantined.
- It allows the administrator to monitor compliance rates and potentially not move to a full enforcement scenario.

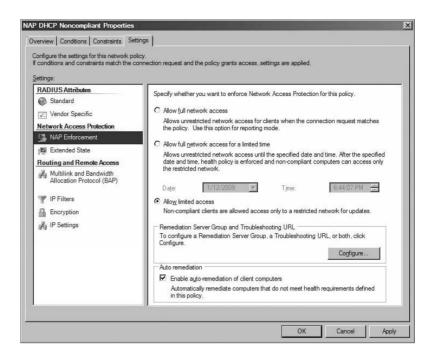
The second point is important because full enforcement can have an impact on your users' productivity and will potentially require additional resources to support.

Full enforcement Full enforcement is the final phase in your NAP deployment, which now will quarantine machines that are not compliant with your patch policy. If you select the Auto-remediation check box, your clients will automatically go to their distribution points to download the patches that are required for network access.

In full enforcement with Configuration Manager, the flow of clients being autoremediated goes like this:

- The client connects to the network, and Configuration Manager sends its health state to the NAP agent, which then sends an SoH to NPS.
- 2. NPS receives the SoH and passes it to the Configuration Manager SHV for evaluation.
- 3. If the client is deemed to be not compliant with the configured patch policy, the Configuration Manager SHV notifies the NPS, and a statement of health response (SoHR) is sent to the NAP agent telling it to quarantine the machine.
- 4. The Configuration Manager SHA on the client downloads the latest system health policy from the Configuration Manager management point server. A local scan of the client computer then runs to identify all the missing software updates according to the system health policy.
- **5.** The Configuration Manager agent will then contact the distribution point and request the missing patches.
- **6.** The distribution point sends the required patches to the client. Upon receipt of those patches, the NAP agent will then query the Configuration Manager 2007 SHA for its state, and the Configuration Manager SHA will give it to the NAP agent who will then create a new SoH and send it to NPS for evaluation.
- 7. NPS receives the SoH and passes it to the Configuration Manager 2007 SHV for evaluation. Evaluation is done, and now the client will be deemed to be compliant with the patch policy. The SoHR that is sent back tells the NAP agent to remove the machine from quarantine. Figure 14.9 illustrates the policy settings in NPS for full enforcement.





It is important to note that the way that a machine is put into quarantine (as defined earlier in this chapter) is unique to the enforcement method you have deployed. The same goes for how a machine is taken out of the quarantine state and given full network access.

In the next sections, we will focus primarily on the noncompliant machine scenario where you have autoremediation enabled with Configuration Manager 2007 and discuss some design points for each enforcement method.

802.1x (Wired or Wireless) NAP with Configuration Manager 2007

As previously mentioned, you can quarantine a machine in 802.1x NAP in two ways:

- Using VLANs on the switch or WAP
- Sending port ACLs to the switch or the WAP

The most common approach in 802.1x NAP is the use of VLANs, since VLANs are a concept that many network administrators are familiar and comfortable with. By contrast, the concept of port ACLs requires more in-depth knowledge of the RADIUS protocol as well as the inner workings of the switch or WAP to which you are sending the ACLs.

For simplicity's sake, let's assume that the default VLAN that your machines will boot into is your corporate network, which has no restrictions. This is a very common customer-deployed scenario that assumes your clients are compliant until they are proven to be otherwise.

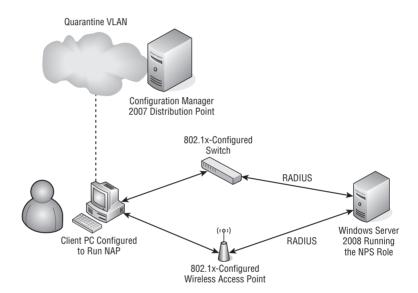
In the VLAN scenario, the first thing you need to understand is that NPS can send back only VLAN tag information to the switch or AP for a single VLAN per policy. This means in NPS when you create your noncompliant policy, only a single set of VLAN tags can be sent to the switch or WAP. Therefore, you can have only one noncompliant, or quarantine, VLAN. Your noncompliant policy with Configuration Manager simply states that if the machine doesn't have

the required patches that you have defined, it must go into the quarantine VLAN. Some people have configured multiple VLANs on their network and may want to have multiple quarantine networks for noncompliant machines, but that is not possible. NPS does allow you to define other conditions in your policies so that you can have more granular access policies, but with the Configuration Manager SHV, either you have the required patches or you do not, plain and simple.

The most common mistake that admins make in deploying Configuration Manager with 802.1x NAP is having the quarantine VLAN locked down too tightly by not having any servers accessible in this network.

With NAP, because you want your clients to autoremediate themselves, you will need to have a distribution point that is accessible in this VLAN so that the noncompliant machines can pull down the required patches for your network. Figure 14.10 illustrates this point.

FIGURE 14.10
The 802.1x quarantine scheme



Similarly, if you are using port ACLs as your means of quarantining your 802.1x machines, the ACL will need to allow TCP traffic to the IP address of the Configuration Manager distribution point.

DHCP NAP with Configuration Manager 2007

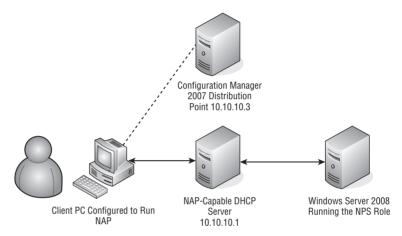
Fortunately, DHCP NAP with Configuration Manager is the simplest of the enforcement methods to deploy and get up and running. Given our assumption that you have a working Configuration Manager environment currently up and running, another inherent assumption is that you have a working IP addressing scheme, which is most likely DHCP-based (unless you have issued static IP addresses to every machine on your network!).

So, if you are doing DHCP on your network (which is probably the case), then you most likely have more than one subnet on your network as well. Given the requirement that your Configuration Manager distribution points must be accessible by your client machines, you most likely have at least one distribution point per subnet deployed, if not more. For DHCP NAP to work with your Configuration Manager environment, that is really the only requirement!

When machines are deemed to be noncompliant in DHCP NAP, they will be issued an IP address from the NAP-enabled scope on your DHCP server (which, if you are implementing DHCP NAP and are in full enforcement, would most likely be all scopes on your DHCP server), but not a default gateway. At the same time, the route table on your noncompliant machines will be modified to allow access only to the remediation servers you have defined in NPS, which in this case are your Configuration Manager distribution points. Figure 14.11 illustrates the quarantine scheme with DHCP.

Because the clients have no default gateway issued to them, you will need to have a distribution point for each subnet that you have.

FIGURE 14.11
The DHVP quarantine scheme



VPN NAP with Configuration Manager 2007

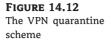
Conceptually, VPN NAP with Configuration Manager 2007 will look and act very similar to DHCP NAP, because the quarantining of noncompliant machines in VPN NAP is done by IP filters.

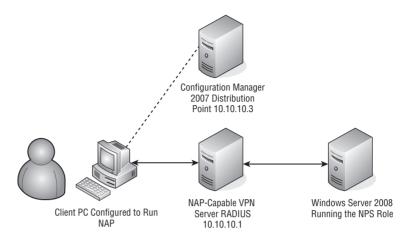
In the NPS policy that you create, by default the IP filters that are sent to the VPN server for connecting clients are the IP addresses of your remediation servers, which in this case are your Configuration Manager distribution points.

Your VPN server typically is configured either as a DHCP relay agent that passes along the client's broadcast request for an IP address or to hand out IP addresses from a predefined pool of addresses that you configure on the VPN server.

If the machine connects to the VPN server and is deemed to be noncompliant to your patch policy, NPS will send down the IP filter list to the VPN server, which will then apply that filter list to that machine's tunnel, which in turn will restrict that machine's access to only your remediation servers. Figure 14.12 illustrates the quarantine scheme with VPN.

One consideration that is unique to VPN NAP is that RADIUS (the protocol used for communication between the VPN server and NPS) has a packet size limit of 4KB. If you have an NPS that has a great many remediation servers defined, the IP filters that will be created can be rather large and possibly take the return packet that gets sent to the VPN server over the 4KB limit, which means that you will have fragmented packets sent to the VPN server. If you have a router that sits between your VPN server and your NPS (which is common), note that some routers may be configured to drop fragmented packets. This would mean that your VPN server may not get the full IP filter list returned to itself, which could also mean that the clients may not be able to communicate with all the remediation servers you defined in your policy.





IPsec NAP with Configuration Manager 2007

IPsec NAP, which is unique to Microsoft's NAP offering in that there are no other known NAC products or solutions that support this, offers the most secure method for NAC as well as the option to encrypt traffic on your network. Although VPN and 802.1x offer the ability to authenticate machines and/or users as they connect to the network (DHCP doesn't have any sort of authentication built into it), IPsec is the only method that allows for the optional encryption of data.

Microsoft also refers to the IPsec technologies as *server and domain isolation* (SDI), primarily because SDI is a less technical term and is actually more accurate in describing what the technology can do.

With IPsec, or SDI, you can logically segment your network by using Active Directory groups or organizational units (OUs) and deploy granular policies that allow machines or users access only to a certain domain or only to certain servers in that domain.

For example, let's say you have an employee who we will call Luke. Luke is a trusted employee who has an Active Directory user account and has a machine that is joined to your domain. Luke's job at your company is as a network engineer, so if you are using SDI, you can then put Luke's account into the proper group in Active Directory that would give him access to most of the network (since he would probably need this type of access as a network engineer), but since Luke is not a member of your Human Resources (HR) group, you can explicitly forbid him to ever connect, or see, your HR servers on the network.

The people in your HR department would also be put into a special group in the Active Directory, and since those employees handle sensitive data (employee addresses, Social Security numbers, and so on), you could have an SDI policy that required any and all traffic between the users in this group (or their machines) to be encrypted.

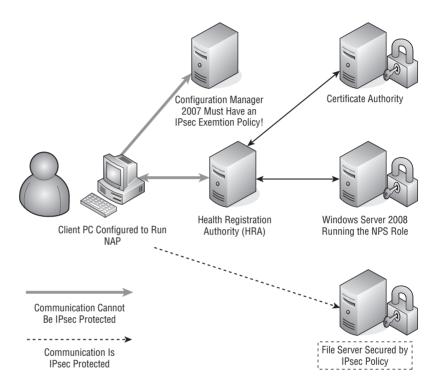
Now that we've gone over the basics of IPsec/SDI, let's look at how this all ties in with your Configuration Manager 2007 infrastructure.

Quarantine in IPsec NAP is done by the NAP agent taking two actions. First, when the NAP agent receives the information in the SoHR that the machine needs to be quarantined, it will immediately delete from the machine store the health certificate that the machine received from the HRA. This will prevent that machine from making any new connections to any machine on the network since those connections will fail without the existence of the proper credentials for the network (that is, the health certificate).

The second action that is taken is that all current SAs that the machine has with other machines on the network are immediately deleted as well, which prevents the machine that has been deemed to be noncompliant from potentially infecting other machines that it has already authenticated itself with.

Figure 14.13 illustrates the IPsec quarantine scheme.

FIGURE 14.13
The IPsec quarantine scheme



When you go to create and apply your IPsec policies for your network, there are two servers that must be exempted from having IPsec required to communicate. The first is your health registration authority (HRA), which is the server that will collect the SoH from your clients and send it to NPS for evaluation. Then, if the machine is deemed to be compliant, it will issue it a health certificate, which is the credential used to authenticate all of your IPsec connections.

Similarly, your Configuration Manager 2007 distribution point must also be exempted from requiring IPsec communications, because this is your remediation server and will need to be able to communicate with noncompliant machines on your network, which in the case of IPsec NAP are machines that do not have a health certificate and therefore cannot do IPsec authentication.

This concept is similar to creating a demilitarized zone (DMZ), which has an external-facing interface that has no protection, or authentication required, but can also have an internal-facing interface so that it can be securely managed by the administrator. This method is a best practice for both your HRA and your Configuration Manager 2007 distribution point in an IPsec NAP-protected network.



AN INTERVIEW WITH BRENT SCALLAN, SENIOR SYSTEM ENGINEER, MICROSOFT CORPORATION

Q: What are the top four preparation steps customers will need to take when integrating NAP and Configuration Manager 2007?

A: Create NAP reports based upon the NPS data that will be collected during a NAP evaluation, which will help measure the success of the Configuration Manager client deployment and software update installations. This data can be compared to the Configuration Manager 2007 reports to understand what the potential impact may be to end users when deferred or full enforcement is enabled and will provide an estimate of how many calls the help desk may expect. These reports should be applicable to any SHA that is planned to be used, including the WSHA that most deployments start out with testing.

Ensure that the Configuration Manager deployment can consistently install software updates on a majority of clients *before* attempting to integrate with NAP. Existing problems in a Configuration Manager 2007 deployment are only highlighted by NAP.

Start planning as early as possible for what exceptions may be needed and how those exceptions will be managed long-term for computers that will not require Configuration Manager to be compliant to pass a NAP health evaluation.

Set expectations with key stakeholders, the help desk, and even end users for how long it can take for remediation to occur for a missing update, especially in the case of a VPN quarantine scenario for a user on a slow link that needs a large update that may also require a reboot to complete. Many end users expect nearly instant remediation for patch installation as compared to turning back on the firewall or some other simple configuration change. We saw most Windows or Office security updates take 6 to 15 minutes over a common VPN connection to be installed and reevaluated to pass the Configuration Manager 2007/NAP evaluation.

Q: What unforeseen issues or problems did you run into during your deployment?

A: We found multiple Configuration Manager 2007 sites in use by domain-joined computers that were unmanaged by us. Site assignments were inconsistent across various deployments/domains and Configuration Manager exceptions were required to be implemented by OUs in addition to security groups. Our multiforest environment required the SMS SHVs to be pointed to a common forest/domain where the Configuration Manager sites also published their health state references. There were challenges in determining which patch was missing from client-side logs.

Q: Are there any best practices that you would recommend when deploying NAP and Configuration Manager?

A: Utilize the Windows System Health Agent (WSHA) to ensure automatic updates are enabled, and deploy the Configuration Manager 2007 client using GPO and WSUS options. Leverage GPO-based site assignment settings for multisite environments. Approve patches for distribution in WSUS so that the Windows Update GUI can be leveraged to determine whether/what updates are missing and whether the client can successfully communicate with the underlying WSUS infrastructure that Configuration Manager 2007 requires.

Q: What additional benefits have you seen in your deployment of NAP and Configuration Manager?

A: NAP provided a very granular audit mechanism for the Configuration Manager 2007 deployment, which exposed issues that previously existed but had not been addressed. Configuration Manager 2007 client installation base and patch compliance increased with NAP deployment. There was a better user experience for compliance validation for scenarios such as NAP/VPN as compared to custom MSIT solutions that leveraged the legacy RQS/RQC features. It also provided the needed framework for additional SHA provisioning and also for requiring non-Microsoft security updates.

The Bottom Line

Identify the components that make up NAP and their roles. NAP as a technology has many different parts associated with it, so understanding the terminology and how the various parts interact is critical to understanding and planning for a successful NAP deployment.

Master It

- What is a system health agent (SHA), and how does this relate to Configuration Manager 2007?
- ◆ What is a statement of health (SoH)?
- What is a system health validator (SHV), and how does this relate to Configuration Manager 2007?

Integrate your choice of the NAP enforcement methods with your current Configuration Manager 2007 deployment. Each of the four enforcement methods discussed in this chapter has a unique way of handling network access as well as of quarantining of machines that become noncompliant. Once you understand the impact of these access and quarantine methods, you will then be ready to start integrating NAP into your Configuration Manager 2007 environment.

Master It

- ◆ How does NAP quarantine noncompliant machines in DHCP NAP?
- ◆ In VPN NAP?
- ◆ In 802.1x (wired or wireless) NAP?
- ◆ In IPsec NAP?

Deploy NAP with Configuration Manager 2007 in a phased approach to minimize your risk. Technologies such as NAP and Configuration Manager 2007 require careful planning and thought around the impact of quarantining machines and then autoremediating them. In some cases, network redesign work may be required for those deployments that are larger and more complex. Having the ability to introduce NAP into your Configuration Manager environment is very beneficial in helping you minimize the impact on the users of your network.

Give a brief description of each of these phases in your answers.

Master It Name the three phases of a successful NAP deployment and one benefit of each phase.

Chapter 15

Troubleshooting

Throughout this book, you have journeyed through all the various aspects of Configuration Manager 2007, and during that journey we have assumed that each of the functions discussed in this book worked flawlessly. However, everyone knows that problems arise and that sometimes things do not go as planned. After all, Configuration Manager 2007 depends on other software, such as SQL Server, IIS, and so on; it also depends on network resources and disk resources. Any of these items can have issues and cause the Configuration Manager 2007 hierarchy not to function as designed.

Although this book cannot cover every scenario that might arise, some great community resources can guide you along your troubleshooting path, including Microsoft TechNet and myIT-forum.com.

In this chapter, we will cover the basics of troubleshooting a Configuration Manager 2007 infrastructure and how to know which log file you should begin looking for first when a problem arises.

In this chapter, you will learn how to do the following:

- Create a basic maintenance plan
- View log files using SMS Trace
- View client status report information

Creating the Maintenance Plan

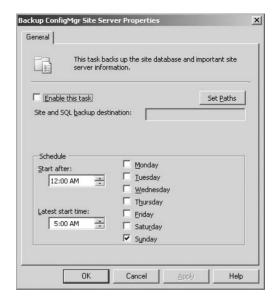
The best way to prevent issues from arising in Configuration Manager 2007 is to create and follow a standard maintenance plan. A well-executed maintenance plan that is followed will allow administrators to be actively aware of their Configuration Manager 2007 hierarchy, offering a better chance of finding possible concerns before they become issues. Proactively watching the environment can reduce the number of major issues and thus keep your environment healthier.

Configuration Manager 2007 has some predefined site maintenance tasks that are enabled by default and some that need to be enabled. To view and modify the site maintenance tasks, take the following steps:

- Open the Configuration Manager console, and expand Site Database; then expand Site Management ➤ Site Code ➤ Site Settings.
- **2.** Under Site Settings, browse to Site Maintenance, and expand it to reveal the Tasks node. By default, Microsoft has 21 predefined tasks. Some of these tasks are enabled, while others are disabled by default.

3. To enable a task, double-click its name to display the task's Properties dialog box. (Figure 15.1 shows the dialog box for Backup ConfigMgr Site Server.) Select the Enable This Task box.

FIGURE 15.1 Enabling the Backup ConfigMgr Site Server task in its Properties dialog box



To ensure the proper health of the site, you should enable some of the predefined Site Maintenance tasks provided by Microsoft, while you'll need to modify the schedule of other tasks. Table 15.1 lists how the tasks should be configured in a typical maintenance plan; this might not be appropriate for all environments, but you can use the table as a guideline.

TABLE 15.1: Site Maintenance Tasks

TASK NAME	ENABLED BY DEFAULT?	SCHEDULE
Backup ConfigMgr Site Server	Yes	Daily
Rebuild Indexes	Yes	Weekly
Monitor Keys	Yes	Weekly
Delete Aged Inventory History	Yes	Weekly
Delete Aged Status Messages	Yes	Daily
Delete Aged Discovery Data	Yes	Weekly
Delete Aged Collected Files	Yes	Weekly
Delete Aged Software Metering Data	Yes	Daily

TABLE 15.1: Site Maintenance Tasks (CONTINUED)

TASK NAME	ENABLED BY DEFAULT?	SCHEDULE
Delete Aged Software Metering Summary Data	Yes	Weekly
Summarize Software Metering File Usage Data	Yes	Daily
Summarize Software Metering Monthly Usage Data	Yes	Daily
Clear Install Flag	No	Weekly
Delete Inactive Client Discovery Data	Yes	Weekly
Delete Obsolete Client Discovery Data	Yes	Weekly
Delete Aged Configuration Management Data	Yes	Weekly
Delete Aged Client Access License Data	No	Weekly
Summarize Client Access License Weekly Usage Data	No	Weekly
Delete Aged Computer Association Data	Yes	Weekly
Delete Aged Delete Detection Data	Yes	Weekly
Reset AMT Computer Passwords	Yes	Weekly
Evaluate Provisioned AMT Computer Certificates	Yes	Weekly

Some tasks do not need to be performed as frequently as others but are important to develop a maintenance plan to ensure the proper health of the site. Table 15.2 summarizes what a typical maintenance plan should be for Configuration Manager 2007. Again, these recommendations might not be appropriate for organizations of all sizes; the table is meant to be used only as a guideline.

TABLE 15.2: Maintenance Plan

TASK	INTERVAL	COMMENTS
Check status messages.	Daily	Check for warnings and errors. They are available in either a web report or within the administrator console.
Check event log on site server for warnings or errors.	Daily	This is the Windows event log.
Check SMS log folders for crash dumps.	Daily	This will help you know whether the site system failed.

TABLE 15.2: Maintenance Plan (CONTINUED)

TASK	INTERVAL	COMMENTS
Monitor site system's inbox folder(s).	Daily	Check this for possible backlogs of files.
Clean out old machines and user accounts.	Daily	Remove old resources.
Check client status.	Daily	
Back up site server to removable media.	Daily	Ensure that the copy of the site backup is moved to removable media such as tape.
Delete unnecessary objects.	Weekly	Remove unneeded collections, packages, programs, advertisements, and queries.
Delete unnecessary files from site systems.	Weekly	Delete unneeded files.
Check disk space on all site systems.	Weekly	
Check advertisement status.	Weekly	View the advertisement report to see whether any older advertisements suddenly are failing.
Defragment all site systems.	Monthly	This can improve site performance.
Review site boundaries.	Quarterly	Ensure that your site boundaries are still valid.
Perform DR test.	Biannual	Ensure that backups actually work.
Review documentation.	Biannual	Confirm that documentation is updated and complete.
Review maintenance plan.	Biannual	Modify the maintenance plan if anything has changed or needs to be added or removed.

Getting an approved maintenance plan for your hierarchy is your first step to developing a solid Configuration Manager infrastructure. The next step is to automate as many of the tasks as possible so they can be done in the most efficient manner without sacrificing the results. A maintenance plan is only as strong as the people implementing the plan.

Using Troubleshooting Tools

The most important troubleshooting tools are log files and status messages.

Log Files

For the majority of troubleshooting, administrators will focus on the log (.log) files on either the client or the server, and in some cases both. The client stores the log files in the folder C:\Windows\System32\ccm\logs, while the site server stores the log files in the folder

<installation Directory>\Microsoft Configuration Manager\Logs. Tables 15.3–15.5 list the
site server log files, management point log files, and client log files, respectively.

TABLE 15.3: Site Server Log Files

SITE SERVER LOG FILE	PURPOSE
Ccm	Records client Configuration Manager tasks
Cidm	Records changes to the client settings by the Client Install Data Manager (CIDM)
Colleval	Logs when collections are created, changed, and deleted by the Collection Evaluator
Compsumm	Records Component Status Summarizer tasks
Csnfsvc	Records Courier Sender information between sites
Dataldr	Processes management information format (MIF) files and hardware inventory in the Configuration Manager 2007 database
Ddm	Saves Discovery Data Record (DDR) information to the Configuration Manager 2007 database by the Discovery Data Manager
Despool	Records incoming site-to-site communication transfers
Distmgr	Records package creation, compression, delta replication, and information updates
Hman	Records site configuration changes and publishes site information in Active Directory Domain Services
Inboxast	Records files that are moved from the management point to the corresponding SMS\INBOXES folder
Inboxmgr	Records file maintenance
Invproc	Records the processing of delta MIF files for the Dataloader component for client inventory files $% \left(1\right) =\left(1\right) \left(1$
Mpcontrol	Records the registration of the management point with WINS and records the availability of the management point every 10 minutes
Mpfdm	Management point component that moves client files to the corresponding SMS\INBOXES folder
Mpmsi	Management point .msi installation log
Mpsetup	Records the management point installation wrapper process

 TABLE 15.3:
 Site Server Log Files (CONTINUED)

SITE SERVER LOG FILE	PURPOSE
Offermgr	Records advertisement updates
Offersum	Records summarization of advertisement status messages
Policypv	Records updates to the client policies to reflect changes to client settings or advertisements
Replmgr	Records the replication of files between the site server components and the scheduler component
Rsetup	Records reporting point setup
Sched	Records files that are sent to other child and parent sites
Sender	Records files that are sent to other child and parent sites
Sinvproc	Records client software inventory data processing to the site database in Microsoft SQL Server
Sitecomp	Records maintenance of the installed site components
Sitectrl	Records site setting changes to the Sitectrl.ct0 file
Sitestat	Records the monitoring process of all site systems
Smsdbmon	Records database changes
Smsexec	Records processing of all site server component threads
Smsprov	Records WMI provider access to the site database
Smsreportinginstall	Records the reporting point installation; this component starts the installation tasks and processes configuration changes
Srvacct	Records the maintenance of accounts when the site uses standard security
Statmgr	Writes all status messages to the database
Swmproc	Processes metering files and maintains settings

TABLE 15.4: Management Point Log Files

MANAGEMENT POINT LOG FILE	PURPOSE
MP_Ddr	Records the conversion of XML $.ddr$ records from clients and copies them to the site server
MP_GetAuth	Records the status of the site management points
MP_GetPolicy	Records policy information
MP_Hinv	Converts XML hardware inventory records from clients and copies the files to the site server
MP_Location	Records location manager tasks
MP_Policy	Records policy communication
MP_Relay	Copies files that are collected from the client
MP_Retry	Records the hardware inventory retry processes
MP_Sinv	Converts XML hardware inventory records from clients and copies them to the site server
MP_Status	Converts $XML.svf$ status message files from clients and copies them to the site server

Note: The default location for the management point log files is Program Files $SMS_CCM \setminus Logs$ on the management point.

TABLE 15.5: Client Log Files

CLIENT LOG FILE	Purpose
CAS	Content Access Service for the local machine's package cache
CcmExec	Tracks the clients activities and SMS agent host service information
CertificateMaintenance	Records Active Directory certificates for the directory service and management points
ClientIDManagerStartup	Used for the maintenance of the resource's GUID
ClientLocation	Tracks the resource's site assignments
ContentTransferManager	Records scheduling information for the Background Intelligence Transfer Service (BITS) or Server Message Block (SMB) to download or to access Configuration Manager packages
DataTransferService	Records all BITS communication for policy or package access
Execmgr	Records advertisement information as advertisements execute

 TABLE 15.5:
 Client Log Files (CONTINUED)

CLIENT LOG FILE	PURPOSE
FileBITS	Records SMB package access tasks
Fsinvprovider	Windows Management Instrumentation (WMI) provider for software
13111vpi ov idei	Inventory and file collection tasks
InventoryAgent	Creates (DDRs) and hardware and software inventory records
LocationServices	Identifies located management points and distribution points
MIFProvider	Identifies the MIF WMI provider
Mtrmgr	Tracks software metering processes
PolicyAgent	Requests policies by using the data transfer service
PolicyAgentProvider	Records any policy changes
PolicyEvaluator	Records any new policy settings
RemCtr1	Logs when the remote control component starts
Scheduler	Records schedule tasks for all client operations
SMSCliui	Records usage of the Systems Management tool in Control Panel
StatusAgent	Logs status messages that are created by the client components
SWMTRReportGen	Generates a usage data report that is collected by the metering agent

There are also log files outside Configuration Manager 2007 that you will need to be aware of when troubleshooting issues within Configuration Manager; Table 15.6 lists them.

TABLE 15.6: Additional Log Files

NAME OR CATEGORY	LOCATION	DESCRIPTION
IIS log files	%windir%\system32\Logsfiles	Log file for Internet Information Services (IIS). Logs HTTP transactions.
SQL log files	SQL Enterprise Manager	Logs SQL activities.
WMI	%windir%\system32\wbem\logs	The WMI repository is the key to the hardware inventory of the clients. Become very familiar with these logs.
SMSAdminUI.log	<pre><install directory=""> \Adminui\Adminuilog\</install></pre>	Logs issues with the Configuration Manager console.

Status Messages

Now that you have seen where the log files reside on both the client and servers, we will cover the troubleshooting components in the Configuration Manager 2007 console. Microsoft has continued to provide status message within the console.

Status messages do have some limitations. The first limitation is that site systems must be able to communicate in order for status messages to be transferred back; if a site system component cannot report back because of a failed network connection, it might still be showing that it is available. Another limitation is that most client messages are transferred as low priority by default, and during high utilizations these messages might be delayed.

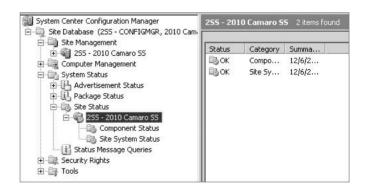
Although status messages have some limitations, they can still be vital weapons in the troubleshooting arsenal of a Configuration Manager administrator. They just shouldn't be the only source for troubleshooting. Status messages reside in one location, which is why they provide some benefit when troubleshooting. They are arranged in one place so you can quickly see the health of the site at a glance.

To view the Site Status dashboard, follow these steps:

- 1. In the Configuration Manager console, expand Site Database ➤ Site Systems ➤ Site Status.
- 2. Expand the site node.

The Site Status dashboard is a summarized collection of the status of all the reported sites for easy viewing and with drill-down abilities for each message. The Site Status dashboard is organized into two categories, Component Status and Site System Status, shown in Figure 15.2.

FIGURE 15.2 Viewing the Site Status dashboard

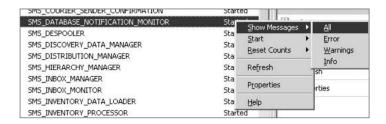


To dig deeper into a Component Status message to see more details about a problem, you can follow these steps:

- 1. In the Configuration Manager console, expand Site Database ➤ Site Systems ➤ Site Status.
- 2. Expand the site.
- 3. Expand Component Status.

- **4.** Select the component you want to investigate. In this example, we will select the component SMS_DATABASE_NOTIFICATION_MONITOR.
- **5.** Right-click the component, and select Show Messages ➤ All, as shown in Figure 15.3.

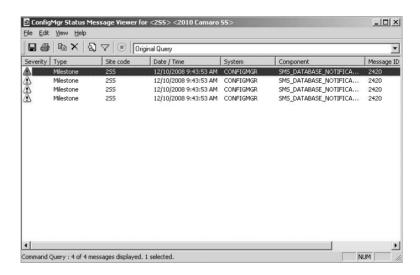
FIGURE 15.3 The Show Messages menu



Note that you can filter the returned messages by selecting All, Info, Warning, or Error Messages.

6. This opens the ConfigMgr Status Message Viewer for *<Site Code> <Site Name>* window, as shown in Figure 15.4.

FIGURE 15.4
The ConfigMgr Status
Message Viewer window



Within the ConfigMgr Status Message Viewer window, you can double-click any of the messages to get a detailed view of the message, as shown in Figure 15.5.

FIGURE 15.5
The Status Message
Details dialog box



USING WEB REPORTS TO VIEW STATUS MESSAGES

You can view status messages from the Web Reports tool within Configuration Manager 2007. This is beneficial in case you are not able to access the Configuration Manager console or you have limited access to it. In either case, you can browse to your Reporting Point web console and view the status messages within a browser.

As discussed in Chapter 11, web reports allow administrators to provide focused views of a Configuration Manager 2007 site database via a web browser and can be set up within a dashboard to give managers an at-a-glance overview of the hierarchy. Table 15.7 lists the reports available in the Status Messages category.

TABLE 15.7: Status Messages Reports

NAME	REPORT ID	DESCRIPTION
All Messages for a Specific Message ID	77	Lists the messages with a single message ID
Clients Reporting Errors in the Last 12 Hours for a Specific Site	79	Lists the computers and components reporting errors in the last 12 hours and the number of errors reported
Component Messages for the Last 12 Hours	87	Lists the component messages for the last 12 hours for a specific site code, computer, and component
Component Messages for the Last Hour (for a Specific Site, Computer, and Component)	86	Lists the status messages created in the last hour by a specified component on a specified computer in a specified SMS site

TABLE 15.7: Status Messages Reports (CONTINUED)

NAME	REPORT ID	DESCRIPTION	
Count Component Messages for the Last Hour for a Specific Site	83	Displays the number of status messages by component and severity reported in the last hour at a single specified site	
Count Errors in the Last 12 Hours	78	Displays the number of server component error status messages in the last 12 hours	
Fatal Errors (by Component)	81	Lists the computers reporting fatal errors by component	
Fatal Errors (by Computer Name)	80	Lists the computers reporting fatal errors by computer name	
Last 1,000 Messages for a Specific Computer (Errors and Warnings)	84	Summarizes the last 1,000 error and warning component status messages for a single specified computer	
Last 1,000 Messages for a Specific Computer (Errors)	82	Summarizes the last 1,000 error server component status messages for a single specified computer	
Last 1,000 Messages for a Specific Computer (Errors, Warnings, and Information)	85	Summarizes the last 1,000 error, warning, and informational component status messages for a single specified computer	
Last 1,000 Messages for a Specific Server Component	88	Summarizes the most recent 1,000 status messages for a single specified server component	

As you can see, Microsoft has provided some nice reports out of the box for status messages. Of course, you can create your own report or modify any of the existing reports to fit your needs.

ADVERTISEMENT STATUS

Configuration Manager 2007 also offers advertisement status messages that show the status of the various advertisements within your enterprise. When you open the Advertisement Status node (by expanding Site Database > System Status > Advertisement Status), Configuration Manager displays a summary view of all your advertisements within the site. Table 15.8 shows the items included in the summary view.

TABLE 15.8: Advertisement Status Summary

COLUMN NAME	DESCRIPTION
Name	Displays the advertisement name
Received	Displays the number of client computers that have received this advertisement
Failures	Displays the number of client computers the advertisement failed
Programs Started	Displays the number of client computers on which the program started
Program Errors	Displays the number of client computers on which the program failed to run successfully
Program Success	Displays the number of client computers on which the program ran successfully
Program Errors (MIF)	If the program generates status MIF files, displays the number of programs that failed to run successfully
Program Success (MIF)	If the program generates status MIF files, displays the number of programs that ran successfully
Package	Displays the package name associated with the advertisement
Program	Displays the program associated with the advertisement
Target Collection	Displays the collection the advertisement is assigned
Available After	Displays when the advertisement is available
Expires After	Displays when the advertisement expires
Advertisement ID	Displays the associated advertisement ID

You can drill down into any of these advertisements by double-clicking its name to see more information about it. Within this window, you are able to view all the messages or display them in a filtered view by selecting Show Messages by All, Received, Failures, Program Started, Program Errors, Program Success, Program Errors (MIF), or Program Success (MIF). Once you select your filtered or unfiltered view, you will be taken to the ConfigMgr Status Message Viewer window as we discussed earlier, but it will be displaying only the information pertaining to the advertisement selected.

PACKAGE STATUS

As with advertisements, Configuration Manager 2007 offers package status messages that show the status of the various packages within Configuration Manager. When you open the Package Status node by expanding Site Database > System Status > Package Status, Configuration Manager displays a summary view of all your packages within the site. Table 15.9 shows the items included in the summary view.

TABLE 15.9:	Package Status Summary
-------------	------------------------

COLUMN NAME	DESCRIPTION
Name	Displays the name of the package
Source Version	Displays the version number of the source files
Version Date	Displays the time and date the package was last changed
Targeted	Displays the total number of distribution points that have a copy of this package
Installed	Displays the total number of distribution points that have a copy of the current version
Retrying	Displays the total number of distribution points that have had a failure in the copying the package but have not exceeded the number of retries allowed and are currently retrying to copy the package or in the state of removing the old package
Failed	Displays the total number of distribution points that have exceeded the number of retries and was unsuccessful at copying the package
Source Site	Displays the site where the package was created
Size	Displays the size of the package source folder
Compressed Size	Displays the size of the compressed version of the package source folder
Package ID	Displays the package ID

Each of these package names can be drilled into by double-clicking the name. You will then be shown more information about the particular package. Within this window, you are able to view all the messages or display them in a filtered view by selecting Show Messages by All, Error, Warnings, or Info. Once you select your filtered or unfiltered view, you will be taken to the Status Message: Set Viewing Period dialog box, shown in Figure 15.6.

This dialog box allows you to set a date and time or select a preset date and time. The viewer will show messages only on or after the time selected, and it will display only the information pertaining to the package selected within the time frame selected.

FIGURE 15.6

The Status Message: Set Viewing Period dialog box



SITE SYSTEM STATUS

The Site System Status home page will highlight all the site systems within your Configuration Manager infrastructure and show a summary of the systems. Table 15.10 displays the information contained when you browse to the Site System Status home page by expanding Site Database ➤ System Status ➤ Site System ➤ Site Code ➤ Site System Status in the Configuration Manager console.

TABLE 15.10: Site System Status

COLUMN NAME	DESCRIPTION	
Status	Displays the status of the Configuration Manager 2007 site and any child site. The status will be OK, Warning, or Critical.	
Site System	Displays the NetBIOS name of the site system.	
Role	Displays the role assigned to the site system.	
Storage Object	Displays the name and location of the storage unit.	
Total	Displays the total available disk space.	
Free	Displays the total available free space.	
% Free	Displays the percentage of available free space.	
Down Since	Displays the time that the site system could not be contacted.	
Availability	Displays if the site system is currently online or offline.	

Because of the slow replication speed of status messages, most Configuration Manager administrators will focus on the log files of the client, the server, and often a combination of both. Because there are so many log files to keep track of which log file contains the information you need for troubleshooting, every Configuration Manager administrator needs two tools. The first is a free download from Microsoft called the Configuration Manager 2007 Toolkit; you can find it here:

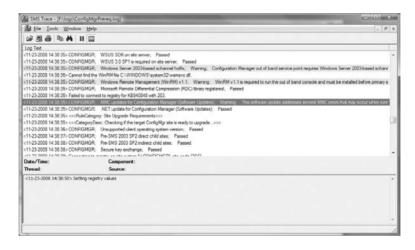
www.microsoft.com/downloads/details.aspx?FamilyID=948e477e-fd3b-4a09-9015-141683c7ad5f&DisplayLang=en

This package contains one of the best tools for reading log files we have seen. Trace32 is a log viewer that constantly monitors the opened file for updates. It provides real-time updates of any log file, allowing administrators to see exactly what is happening on a client or site system. If that isn't enough to win you over, Trace32 includes the capability to highlight and filter features to allow at-a-glance log viewing. Finally, the tool includes an error code dictionary, shown in Figure 15.7, so that you can quickly translate most of Microsoft's decimal error codes into something meaningful and useful right within the tool. For example, entering 5 in the error lookup window utility returns "Access Denied." This feature is available by selecting Tools > Lookup in the Trace32 utility. Trace32 will highlight errors, as shown in Figure 15.8, so they stand out.

FIGURE 15.7
Trace32 error lookup



FIGURE 15.8 Highlighting errors in Trace32



The other tool you need to have is a reference tool for all the log files. The log files and their locations were covered earlier in this chapter and will be a great reference tool, so now you are well equipped to handle troubleshooting a Configuration Manager 2007 site either using the log files from the client or site systems, using the status messages in Configuration Manager, or using the web reporting feature of Configuration Manager.

Troubleshooting Configuration Manager Deployment

If you experience issues deploying Configuration Manager 2007, you should first look into the following areas to see whether the issue is related to permissions, disk space, network connectivity, or timing.

Permissions are extremely important to Configuration Manager deployment. If Configuration Manager does not have appropriate rights to make the connection, then the operation will fail. Admins using the Configuration Manager console will need the appropriate permissions for WMI, for DCOM, for NTFS, and, lastly, within Configuration Manager itself.

Disk space is used to store the site database, packages, software updates, inventory, and collected files; all of this can use up a lot of disk space. How much space is used depends on your environment, but you should always verify you have sufficient disk space to store all the data within Configuration Manager.

Network connectivity is a key requirement of Configuration Manager. The site system must be able to communicate with other site systems and clients. As stated earlier, sometimes the network connectivity might be down but the status messages have not updated, so you need to ensure the clients and servers can connect to each other.

Patience is not always a trait that Configuration Manager administrators have, but it is an important one to develop. Some tasks within Configuration Manager, Active Directory, and Windows in general just take some time to complete; it's a process. That is why examining the log files is so important.

Troubleshooting the Configuration Manager Console

Typically any issue you have connecting to the Configuration Manager 2007 console involves or is related to permissions. So, check the account, and ensure that the user is a member of the appropriate group (by default the SMS Admins group) or has equivalent rights.

Troubleshooting issues with the Configuration Manager console should begin in the SMSAdminUI.log file. As noted earlier, this log file does not reside with the other log files. Instead, it resides in the <installation directory>\AdminUI\adminUILog directory on the workstation where the Configuration Manager console is installed.

By design, you see only the objects within the Configuration Manager console to which you have rights. Resolving this issue requires that someone with administrative rights to the object grant you permission to the instance or class that you need to manage.

Microsoft provides a way to open the Configuration Manager console using verbose logging. This is extremely helpful when troubleshooting issues with the console. Take the following steps to enable verbose logging:

- Browse to the <installation directory>\AdminUI\bin folder, and edit the adminui.console.dll.config file using your favorite text editor.
- 2. Modify the following line:

```
<source name="SmsAdminUISnapIn" switchValue="Error" >
to this:
    <source name="SmsAdminUISnapIn" switchValue="Verbose" >
```

3. Restart the console.

- 4. Examine the SMSAdminUI.log file.
- 5. Reset the switchValue value in adminui.console.dll.config to "Error". This will reduce the extra overhead on the system created when the value was set to "Verbose".

Troubleshooting Clients with the Client Status Tool

Clients can become your main source of pain, but learning where to go when problems arise will help you quickly resolve any issues that could creep into your environment.

Client Status Reporting

With Configuration Manager 2007 R2, Microsoft released the client status reporting feature, which (as discussed in Chapter 4) evolved from the old SMS 2003 Client Health Monitoring solution. Client status reporting allows Configuration Manager 2007 to provide up-to-date information on the status of its clients. Prior to Configuration Manager 2007 R2, a Configuration Manager administrator could use the built-in web reports to check the health of a client; however, it was never possible to get up-to-date information about the status of the clients. Now, client status reporting provides tools and resources to help monitor the status of clients within your organization. It enables you to identify clients that are in any of the following states:

- Online but not requesting policy
- ◆ Online but with nonfunctioning client components
- Online but lacking up-to-date discovery or inventory
- Offline

It also provides some new reports.

Client Status Reporting Prerequisites

Client status reporting has some prerequisites that you need to take into consideration before implementing this feature. Table 15.11 shows all the prerequisites for this feature.

TARLE 15.11:	Client Status Reporting Prerequis	nit on
TARLE ID II!	Lilent Statils Reporting Prefection	29112

Prerequisites	More Information
Configuration Manager 2007 R2	Client status reporting is not compatible except on Configuration Manager 2007 R2.
Reporting point site system	The reporting point site system must be installed prior to installing client status reporting.
Client system reporting host system must be running Microsoft .NET Framework 2.0	This is the computer on which the client status reporting feature is installed.
Office web components installed	Some reports for client status reporting contain charts that require the Office web components.

Installing and Configuring Client Status Reporting

Client status reporting is available in the R2 installation, but it's not installed by default when R2 is installed. Chapter 4 detailed the steps for installing and configuring client status reporting, but we'll quickly summarize them here:

- 1. From the R2 installation media, browse to the Client Status Reporting folder, and run the ClientStatusReporting.msi file.
- 2. On the Client Status Reporting Wizard's Welcome page, click Next.
- 3. On the License Agreement Page, you'll need to accept the license; then click Next.
- **4.** This will present you with the Destination Folder page. Change the path, if desired, and click Next.
- **5.** On the installation screen of the setup wizard, click Next.
- **6.** The installation will not take very long, and you will be presented with the Setup Complete dialog box. Click Finish.

Now client status reporting has been installed on your Configuration Manager 2007 R2 server and is ready to configure. Take the following steps to configure client status reporting:

- From the Start menu, browse to the Microsoft Configuration Manager 2007 R2 client status reporting feature, and click Configure Status Reporting to display the Configuration Manager 2007 client status reporting configuration tool.
- On the Site Settings tab, fill in the ConfigMgr SQL Server and instance information along with the ConfigMgr site database. Also, choose to use a local system account, or specify an account.
- **3.** On the Options tab, you can configure the time frame in which a client computer must have reported data to be considered active. The default value is seven days.
- **4.** On the Scheduling tab, you can specify whether the client policy can request information from the management points and set a schedule for the request to run. This tab also allows you to schedule a ping of inactive clients. A client status reporting client ping performs not only the standard ping commands but also checks the state of the Configuration Manager 2007 client service and BITS. The clients marked as inactive will be pinged following the schedule you specify here.
- **5.** The Info tab displays the version, status, and details about the service.

Importing and Viewing the Client Status Reports

After client status reporting is installed and configured, you will need to import the reports from the ClientStatusReports.mof file, located in the Reports folder of your installation directory, for example:

C:\Program Files\Microsoft ConfigMgr Client Status\Reports

Then follow these steps:

- 1. To import the file, open the Configuration Manager 2007 console, and expand Site Database ➤ Computer Manager ➤ Reporting ➤ Reports.
- 2. Right-click Reports, and select Import Objects.

- **3.** On the Import Object Wizard's Welcome page, click Next.
- **4.** On the Import Object Wizard's MOF File Name page, browse to the location of the ClientStatusReports.mof file, and click Next.
- 5. The Objects page lists the six new reports contained in ClientStatusReports.mof. Click Next, and click Next again on the (currently blank) Comments page.
- Finally, the Completing the Import Object Wizard page appears, showing that you have successfully completed the Import Object Wizard.

The Configuration Manager 2007 console now has the new reports under the Client Status category. Table 15.12 describes the six new reports and the information they provide.

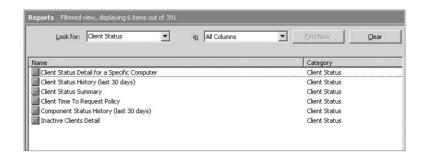
TABLE 15.12:	Client Status Reports
--------------	-----------------------

REPORT NAME	DESCRIPTION
Inactive Clients Detail	This report provides a detailed list of clients that don't have a policy, updated hardware or software inventory, and have no current DDR or status messages in the database. For large sites, results can be reduced to only a top percentage of inactive clients. All times are displayed in UTC.
Client Status History (Last 30 Days)	This report provides a historical view of the overall client status in the environment for the past 30 days.
Client Status Detail for a Specific Computer	This report provides the client status data for a specified computer.
Component Status History (Last 30 Days)	This report provides administrators with a gauge to determine how core client activities including policy requests, heartbeat (DDR), inventory, and status messaging are performing in their environment.
Client Status Summary	This report provides a summarized view of the overall status of client activity as well as a summary for each client component. Client and agent status is determined by the Client Status Calculation setting (number of days) in the client status reporting feature.
Client Time to Request Policy	This report shows the total number of clients that have requested policy at least once in the last 30 days. Each day represents a total of all clients that have requested policy since day 1 in the cycle. This is useful for determining the time it would take to distribute a policy update to your client population. Client deployments or changes in client count can affect the accuracy of the report.

To view the reports at any time, follow these steps:

- **1.** Open the Configuration Manager 2007 console.
- Expand the Site Database ➤ Computer Management ➤ Reporting ➤ Reports node to display a list of all the reports within your site.
- **3.** Using the built-in filtering tool, type **Client Status** in the Look For text box, as shown in Figure 15.9. Then click Find Now.

FIGURE 15.9
Finding the client status reports in the Reports node



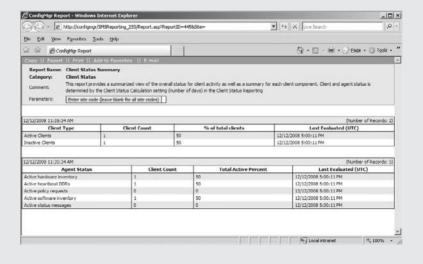


"WE NEED TO KNOW THE HEALTH OF CONFIGURATION MANAGER 2007 CLIENTS."

George T. Management has read a report saying that unhealthy clients can cause unexpected results on the network, so he comes into your office and requests an overview of the health of the clients within Configuration Manager 2007.

After hearing this request and trying to generate a report on your own, you remember that you recently installed client status reporting within your organization. So, you open the report called Client Status Summary by opening the Configuration Manager console and expanding Site Databases > Computer Management > Reporting > Reports.

You print the report and take it to George T. Management. Knowing that Mr. Management will want more information than his initial request, you print each of the reports under the category Client Status and take them with you just in case.



The Bottom Line

Create a basic maintenance plan. Setting up a basic maintenance plan is a vital step to ensure the proper health of your Configuration Manager 2007 hierarchy.

Master It How do you create a basic maintenance plan?

View log files using SMS Trace. Although using SMS Trace to view log files is not a requirement for viewing log files, it is highly recommended because SMS Trace constantly monitors the opened file for updates.

Master It Using SMS Trace to view log files.

View client status report information. One of the advances in Configuration Manager 2007 R2 is the release of client status reporting. Once the feature has been successfully installed and configured, it contains some reports that will help administrators develop a healthy Configuration Manager environment.

Master It View client status reporting reports from the Configuration Manager 2007 console.

Chapter 16

Disaster Recovery

No matter what kind of hardware you are using for your Configuration Manager sites, there is always the possibility that hardware or some other failure will bring a site down.

The only thing you can really do to prepare for something like this is to back up Configuration Manager the best you can so that your site will get back up and running as soon as possible.

Fortunately, Microsoft continues to provide the options that are present in earlier versions of Configuration Manager, and it provides a specialized set of backup and recovery options that you will need to recover your sites quickly.

Configuration Manager primary sites store a large amount data, most of it in the site server's registry, system files, and the Microsoft SQL 2005 site database. A site will operate properly only if all of these sources of data are synchronized.

To make sure that you are getting a complete backup of your Configuration Manager sites, you need to configure the Backup ConfigMgr Site Server maintenance task for at least each primary site and optionally for your secondary sites. This task creates a complete backup snapshot of the data sources that are needed to perform recovery with the Site Repair Wizard, the only way to guarantee that the data sources will be in synch and no data on the server corrupted.

In this chapter, you learn to:

- Configure backups for Configuration Manager sites
- Restore Configuration Manager sites
- Archive backup snapshots to another location

Planning for Disaster Recovery

Planning for disaster recovery in Configuration Manager 2007 is not complicated, but as you'll see in the section "Recovering Configuration Manager," it is a bit different than it was in SMS 2003. With that in mind, you should consider the following when you are planning to set up your backup and recovery plans for your Configuration Manager hierarchy.

◆ The Configuration Manager backup task uses the Volume Shadow Copy Service (VSS), which is a part of Windows Server 2003 and is configured during the installation of Configuration Manager, to make its backup snapshots. Microsoft describes VSS as "a framework which facilitates communication between applications, storage subsystems, and storage management applications (including backup applications) in order to define point-in-time copies of storage data." The shadow copies that are made from VSS of the site server and the site database information are used to back up and restore Configuration Manager sites. By using VSS, the Backup ConfigMgr Site Server maintenance task can keep server downtime for backups to a minimum.

- A complete backup of a Configuration Manager site server needs to include the following:
 - ◆ The Configuration Manager site database (SQL)
 - The folder in which Configuration Manager was installed
 - ◆ The master site control file, which is

<ConfigMgr Install folder>\Inboxes\Sitectrl.box\Sitectrl.ct0

- ◆ The SMS and NAL registry keys on the site server
- Configuration Manager Site systems may contain site data that can be easily recreated if the site fails and isn't backed up during the backup process. Things such as distribution points, management points, reporting points, and server locator points can all be reinstalled when a Configuration Manager site is recovered, so there really isn't a need to back them up.
- Unlike most other SQL applications, the master SQL database isn't needed to restore a Configuration Manager site, so it isn't backed up with the Configuration Manager database when the Backup ConfigMgr Site Server maintenance task is run.

Backing Up Configuration Manager

The first thing to know about backing up Configuration Manager sites is that you can automate the procedure by scheduling the Backup ConfigMgr Site Server maintenance task. We will cover this maintenance task in more detail later in the chapter.

When the Configuration Manager backup service (SMS_SITE_BACKUP) starts, it uses instructions in the backup control file, located at

<ConfigMgr Install Location>\Inboxes\smsbkup.box\smsbkup.ctl

This file can be modified in Notepad to change what the backup service takes a snapshot of, but it isn't usually necessary.

Information on the site backup process is written to the smsbkup.log file, which can be found in the default location for log files, and in the location that is designated in the Backup ConfigMgr Site Server maintenance task when the task is run.

It is important to remember that only site backups created by the Backup ConfigMgr Site Server maintenance task are supported for recovering Configuration Manager sites with the Site Repair Wizard, a procedure we will describe in detail later in this chapter.

Backup Considerations for the Central Site

The process of backing up and recovering a central site is pretty much the same as with any primary site (discussed shortly), but there are special considerations to keep in mind when you back up and restore central sites that make them different than other primary sites when setting up backups of the central site, and when you recover them:

• The central site is the busiest site in your hierarchy, which gives you a smaller time frame for scheduling a backup. Configuration changes are made on a constant basis, and you will probably not be able to recover them all.

- The central site has the largest amount of data, so it is going to take longer to back up than the rest of your primary sites.
- ◆ The central site doesn't have a parent site where it can pull a copy of the site control file.

These combined factors might make you consider backing up less frequently than your other primary sites. Doing this is not a good idea, as the central site is the most important site in your Configuration Manager hierarchy. If one of your primary sites fails, and for some reason your backups for that site are corrupted, you can always use your central site as a source to restore the failed primary site because all data from it is forwarded up and consolidated at the central site. That's not the case with the central site itself. With this in mind, we recommend scheduling the backups of your central site to run every day.

You can take several steps that will enable you to recover as much of your central site as possible in the event of data loss.

- Back up the central site every day.
- Have a reference site for the central site so that recovery tools will be able to recover packages and advertisements that are created after the site is backed up.
- Keep a copy (as recent as possible) of the central site's site control file in a remote location, or reference site.
- Between backup cycles, back up the central site control file as frequently as possible. You
 can use any system tools or batch files that you want to do this. You can also use the Hierarchy Maintenance tool as well.
- Store the backup of the site control file in the *.CTO format so that all you will need to do is rename the file and put it in the right folder on the central site that you are recovering.

With these steps, you should be able to recover most of the central site without too much trouble. You will be able to recover configuration data and software distribution objects from the reference site and the administrative data that might be lost will be regenerated after the central site is back up and running.

Copying Site Backups to Another Location

The first time the Backup ConfigMgr Site Server task runs, it creates a backup snapshot, which can be used to recover a Configuration Manager Site system when it fails. The next time that the backup task runs, it makes a new backup snapshot that will overwrite the one that was made during the last snapshot. This could be a problem if the current backup snapshot becomes corrupt for some reason, as there will not be another backup to restore from.

For that reason, Microsoft recommends that you archive the backup to another location off of the site server itself. As a best practice, it also recommends having multiple backup archives, for the following reasons:

- It is common for backup media to fail, get misplaced, or contain only a partial backup.
 Recovering a failed site from an older backup is better than recovering with no backup at all.
- ◆ A corruption in a site can go undetected for several backup cycles. You may need to go back several cycles to the backup snapshot from before the site became corrupted.

◆ The site might have no backup at all if, for example, the Backup ConfigMgr Site Server task fails. Because the backup task removes the previous backup snapshot before it starts to back up the current data, there will not be a valid backup snapshot.

Archiving the Backup Snapshot to Another Server with AfterBackup.bat

The AfterBackup.bat file has two primary functions:

- Archive a copy of the latest backup to a remote location off of the Site Server that is being backed up.
- Copy that backup in such a way that there are multiple archived copies of site server backups, in case one is corrupted or one of the backup cycles fails.

Microsoft has included support for a batch file appropriately called AfterBackup.bat to run tasks on the site server after the backup task is complete. After successfully running the Backup ConfigMgr Site Server maintenance task, ConfigMgr will try to run this batch file. This batch file is not installed during site setup and will have to be created manually by an administrator after a site server is configured.

If the AfterBackup.bat file exists and is stored in the correct folder on the site server, the batch file will run automatically after the backup task is complete. The AfterBackup.bat file allows you to include commands that will archive the backup snapshot to a location off the server at the end of the backup operation and to perform other post-backup tasks if you include them in the batch file.

The AfterBackup.bat file integrates the archive and backup operations, thus ensuring that every new backup is archived. If the batch file does not exist, it has no effect on the backup success, but in order to archive the backup snapshot, you must use another method.

Although the AfterBackup.bat file is intended to archive backup snapshots, you can include commands in that batch file that will run after every backup, like SQL Server DBCC tests to verify database integrity, or any other health checks on the site server.

As noted, the AfterBackup.bat file isn't created for you when ConfigMgr is installed, and the ConfigMgr documentation does not explain how to set up the AfterBackup.bat file to be able to accomplish this task.

There are several ways to do this (including using third-party tools), some more complicated than others, but probably the simplest way is to use the Windows command xcopy:

```
xcopy "[location of backup files on site server]\*.*" "\\[off site location] \\DATE\\[sitecode]Backup\\*.*" /E /0 /C
```

Add this command to an ASCII file and name it AfterBackup.bat; then place the batch file in the following location:

```
[Drive where ConfigMgr is installed]\ SMS\inboxes\smsbkup.box
```

This isn't the perfect solution, but it will get the job done. One of the drawbacks of archiving this way is that the files will be copied over the network uncompressed to your remote file location. Depending on the size of your ConfigMgr database, archiving may take a long time and might use up a lot of bandwidth if your remote location is on a slow link.

With that in mind, you can also add commands to the AfterBackup.bat file to use file compression software such as WinZip or PKZip to compress the backup files before they are copied to the remote archive location.

WINDOWS APPLICATION LOG ENTRIES CREATED BY THE BACKUP PROCESS

The Backup ConfigMgr Site Server task will write backup status messages to the Application Event Log. Table 16.1 shows a list of the events and their event IDs that are written to the Event Log, as described in the Microsoft documentation.

TABLE 16.1: Configuration Manager Backup Event Log Entries

EVENT ID NUMBER	MESSAGE
5505	SMS Site Backup task is starting. This task will interact with the windows VSS services and the appropriate writers to create a volume snapshot and then back up the required files to the specified destination.
6829	SMS Writer is about to stop the SMS Services as part of the preparation of the SMS Site backup.
3197	1/O is frozen on database SMS_[site code]. No user action is required. However, if I/O is not resumed promptly, you may cancel backup.
3198	1/O was resumed on database SMS_[site code]. No user action is required.
18264	Database backed up.
6830	Component SMS_SITE_VSS_WRITER on computer [site server] reported: the snapshots of the volumes required for the SMS backup have been successfully created.
ID6831	SMS Writer has started the SMS Services successfully.
5056	SMS Site Backup is starting to copy the files from the snapshot.
5057	SMS Site Backup has successfully completed copying the files from the snapshot.
6833	SMS backup task has completed successfully.

Configuring the Backup ConfigMgr Site Server Maintenance Task

The Backup ConfigMgr Site Server maintenance task backs up a Configuration Manager site, including the site database, files, registry keys, and system configuration data. The Site Repair Wizard does not support using third-party tools to back up your Configuration Manager site; it will only use backups made by the Backup ConfigMgr Site Server maintenance task.

BACKING UP A PRIMARY SITE

Before you start to configure the Backup ConfigMgr Site Server maintenance task, make sure that you have Read or Modify permission for the site security object class or instance. Once that is done, do the following:

- In the Configuration Manager console, go to System Center Configuration Manager ➤ Site
 Database ➤ Site Management -<site name> ➤ Site Settings ➤ Site Maintenance ➤ Tasks.
- **2.** Right-click the Backup Site Server task, and then click Properties. The backup task is shown in Figure 16.1.

FIGURE 16.1
The Backup Site
Server task



3. Specify the backup destination folder in local format (C:\ConfigMgrBkup) or in UNC format (\\server\share). If that path doesn't exist, the backup task will create it when it runs. If you set this path up in the install folder for Configuration Manager, the backup will fail. Try to configure backup times during a period when your Configuration Manager site is less active. After you are done, click OK.

TESTING WHETHER SITE BACKUPS ARE WORKING

As soon as you set up the backup maintenance task on a site, you should let it run for the first time and verify that it is running. That way, you won't be surprised to find yourself without a good backup if you have to restore one of your site servers.

The first thing to look for is that the time stamps on the files in the backup folder you set up match the last time the Backup task should have run. If they don't, you should look at the status of the SMS_SITE_BACKUP component for warnings and errors. To do this, follow these steps:

In the Configuration Manager console, go to System Center Configuration Manager ➤ Site
 Database ➤ System Status ➤ Site Status ➤ <site name> ➤ Component Status.

- 2. In the results pane, right-click SMS_SITE_BACKUP, click on Show Messages, and then on All. If you don't see SMS_SITE_BACKUP in the results pane, double-check to see if it is enabled.
- **3.** This will bring up all the status messages for that component for the last 12 hours. If there are any warnings or errors, you can easily find them in the list by their icon.
- **4.** Review all errors and warnings that you see, and they should give you an idea of what the problem is.

COMMON BACKUP TROUBLESHOOTING METHODS

If the previous tests don't help you figure out what is causing the problem with the backup, you can look for errors in a few additional places:

- ◆ Look in the Event Viewer Logs for any account and/or access violations.
- ◆ The SMS_SITE_BACKUP runs under the local system account. Make sure that this account has access to any remote locations in the SMS Backup control file, and that this account has the rights to perform the tasks in the control file's [Tasks] section.
- If you have enabled the SMS_SITE_BACKUP log, check that log for errors. It can be found at

<Configuration Manager installation directory>\Logs\smsbkup.log

HOW TO BACK UP A SECONDARY SITE

Secondary sites can fail, too, and depending on your Configuration Manager hierarchy, and what you are using it for, you may want to back up your secondary sites along with your primaries. You can back up your secondary sites just as you do your primaries, with the Backup Secondary Site Server maintenance task.

The biggest difference between backing up a secondary site and a primary site is that there is no SQL database to back up. There are some other differences:

- ◆ The Backup task will skip the following entries in the backup control file:
 - ◆ Any database commands, such as smssqlinfo and sitedbdump
 - All backup commands that are in the [Tasks] section, in which the <source> is a
 database server.

To back up a secondary site, follow these steps:

- In the Configuration Manager console, go to System Center Configuration Manager ➤ Site
 Database ➤ Site Management ➤ <site name> ➤ <secondary site name> Site Settings ➤ Site
 Maintenance ➤ Tasks.
- 2. Right-click on the Backup Secondary Site Server task, and then click Properties.
- 3. Configure the task as you want it, and then click OK.

Restoring Configuration Manager

Besides getting a failed site up and running again, recovery of a Configuration Manager site is also required if that site is installed with a site code or site server name that has already been used in

the hierarchy. Repairing and re-synchronizing data is what site recovery is designed for, and it is required in order to avoid interruption of operations and corruption of data.

Configuration Manager provides several recovery and repair tools to help you quickly and consistently complete the tasks that are essential to restoring Configuration Manager site operations. These tools allow you to carry out recovery and repair commands that will override existing configuration settings without having to directly access low-level data, as well as to start operations that are not available through other methods.

Understanding the Effects of a Site Failure

Configuration Manager is made up of various site systems and clients. Each site has at least one site system — namely, the site server. The site server will monitor and manage the Configuration Manager site. Each Configuration Manager site also has a site system that is the site database server, and at least one site system that acts as a management point. As we have already established in previous chapters, the management point is the site system that allows the site server and the site's clients to communicate properly.

Along with these important site systems, a site can have any number of additional site systems that perform different roles for a site hierarchy. The site server or any of its site systems can fail, and then they would not be able to provide the services they normally do. If more than one site role is installed on the same server and it fails, then all the services provided by that server will become unavailable. Table 16.2 is a table from Microsoft's documentation on ConfigMgr that shows the results of various site systems becoming offline or otherwise unavailable.

The Site Repair Wizard

The Site Repair Wizard in Configuration Manager is designed to perform complex recovery tasks that would be too difficult or even impossible for an administrator to do by hand. The Site Repair Wizard is installed during Configuration Manager Setup on any computer that has the Configuration Manager console and can be found in the Start Menu. You can also access it from the Configuration Manager console by right-clicking on a site and selecting Repair Site. When you run the Wizard, it logs the site repair information to the RepairWizard.log file. This file is created in the folder

<Configuration Manager install drive>\Program Files\AdminUI\AdminUILog

when the Site Repair Wizard is started. Make sure that you don't try to use the Configuration Manager version of the Site Repair Wizard to repair a SMS 2003 site, and vice versa. You should always use the version of the tool that comes with the version of SMS you are trying to repair.

PRIMARY FUNCTIONS OF THE SITE REPAIR WIZARD

The Site Repair Wizard is designed to make recovering a Configuration Manager site as easy as possible, while also minimizing downtime. The Site Repair Wizard performs these functions when it is used:

- 1. Shut down the site and all of the site systems associated with that site.
- Restore the site database, registry, and site server files from backups that are created by the Backup ConfigMgr Site Server maintenance task.
- Synchronize and reset transaction serial numbers.
- **4.** When possible, recover changes made since the site backup used for recovery was made.

- **5.** Prompt the administrator for certain changes made since the backup that is being used was made.
- **6.** Restart the site.

TABLE 16.2: Results of Configuration Manager Site Failure

			_	
SITE SERVER	SITE DATABASE	MANAGEMENT POINT	DISTRIBUTION POINT	RESULT
Offline	Online	Online	Online	No site administration will be possible, including creation of new advertisements. The management point will collect client information and cache it until the site server is back online. Existing advertisements will run, and clients can find distribution points.
Online	Offline	Online	Online	No site administration will be possible, including creation of new advertisements. If the Configuration Manager 2007 client already has a policy assignment with new policies and if the management point has cached the policy body, the client can make a policy body request and receive the policy body reply. No new policy assignments requests can be serviced. Clients will be able to run programs only if they have already been detected and the associated source files are already cached locally at the client.
Online	Online	Offline	Online	Although new advertisements can be created, the clients will not receive them until a management point is online again. Clients will still collect inventory, software metering, and status information and store them locally until the management point is available. Clients will be able to run programs only if they have already been detected and the associated source files are already cached locally at the client.
Online	Online	Online	Offline	Configuration Manager 2007 clients will be able to run advertisements only if the associated source files have already been downloaded locally.

OVERVIEW OF THE SITE RECOVERY PROCESS

The Site Repair Wizard recovers a Configuration Manager site in two phases: *restore* and *repair*. In the restore phase, the Site Repair Wizard stops the WMI service and all of the Configuration Manager services running on the site server. The site backup snapshot created by the Backup ConfigMgr Site Server maintenance tasks is then restored to the site server. During this phase, you

have the option to restore the site manually (if for some reason you don't have a viable backup, or previous attempts at automatic updates failed) or let the wizard do the restore tasks for you.

In the repair phase, the Site Repair Wizard will repair the recovered Configuration Manager hierarchy, recover objects that might have been created after the site was last backed up (collections, packages, and so on), and then restart all of the site's services.

You can run the Site Repair Wizard more than once on a restored site, in order to complete failed attempts at repairing a site, and you can also just start over if things don't work as they should. The Site Repair Wizard supports restoring a 32-bit operating system backup to a server with a 64-bit operating system, but it does not support restoring a 64-bit operating system backup to a server running 32-bit operating systems.

The Site Repair Wizard also keeps a record of the last time it was run on a Configuration Manager site. This record determines how the Site Repair Wizard is started the next time it is used.

- If the site repair succeeded on the last run, you are notified and given the option to run the Site Repair Wizard over from the start.
- If the last site repair failed, or was cancelled before the repair phase finished, then you are given the option to start the repair where it left off.
- If a repair failed, or was stopped during the restore phase, the Site Repair Wizard will start
 the process from the start.

The Hierarchy Maintenance Tool (Preinst.exe)

The Hierarchy Maintenance tool is used to pass commands to the Configuration Manager Hierarchy Manager Service, which is a thread of the SMS_EXECUTIVE service.

This tool is automatically installed with Configuration Manager and can be found in the folder

<ConfigMgr Install Driver>\Program Files\Microsoft Configuration Manager\bin
\i386\<language code>

on the site server and also in the \SMSSETUP\BIN\I386\<\?1 anguage code> of the Configuration Manager install DVD.

You can use the Hierarchy Maintenance tool to diagnose problems in a site, repair a site, or stop a Configuration Manager completely. To run the Hierarchy Maintenance tool, you must have administrative rights to the computer it is run on, and you must also explicitly have the Site Administer security right; just being part of a group that has that right isn't enough. We will go into detail on how to use this tool later in the chapter.

Recovering Configuration Manager

There are some differences between recovering a ConfigMgr site and recovering SMS 2003 sites. The most notable of these is that the Recovery Expert Wizard has been discontinued and all the manual tasks from it have been incorporated into an improved Site Repair Wizard.

How to Start the Site Repair Wizard

There are two ways to start the Site Repair Wizard:

- From the Configuration Manager console
- ◆ From the Configuration Manager 2007 program group on the Start menu

To open the Site Repair Wizard from the ConfigMgr console, do the following:

- In the console, go to the System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ [Site Name].
- 2. Right-click [Site Name] and then click Repair Site.
- **3.** After the Site Repair Wizard starts, make sure to close the ConfigMgr console before you continue. The Site Repair Wizard will produce an error if you try running it with an MMC console open.

You should open the Site Repair Wizard from the ConfigMgr console only to repair the local site server, on which you've opened the wizard. You can't open the Site Repair Wizard on remote site servers using this method.

To start the Site Repair Wizard from the Start Menu, click Start ➤ Microsoft System Center ➤ Configuration Manager 2007, and then click the ConfigMgr Site Repair Wizard icon.

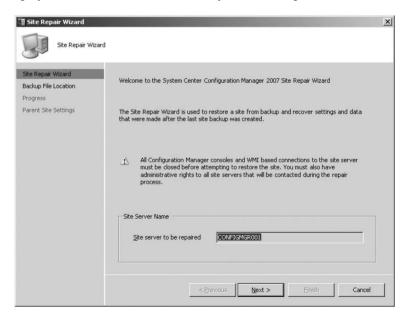
Recovering a Central Site

Once you have started the Site Repair Wizard, you can start recovering your ConfigMgr Site with the wizard's options.

To restore a central site using the Site Repair Wizard, do the following:

1. On the Site Repair Wizard Welcome page, shown in Figure 16.2, make sure that Site Server To Be Repaired displays the name of the site server that you need to repair, and click Next.

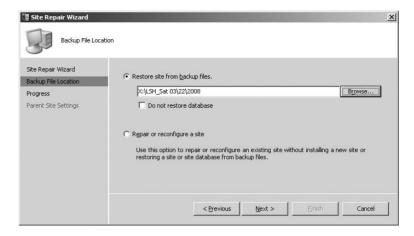
FIGURE 16.2
The Site Repair
Wizard Welcome page



- **2.** On the Backup File Location page, shown in Figure 16.3, click Browse to open the Browse for Folder dialog box, and browse to the location of the most recent backup snapshot.
 - When you do this, make sure you point to the folder containing the subfolder that has the same name as the folder specified in the Backup ConfigMgr Site Server maintenance task,

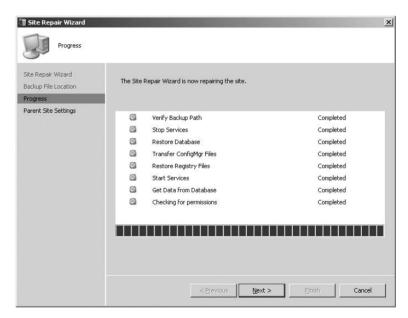
or you will get an error. If you are only trying to recover lost site settings and not the site database, check the Do Not Restore Database option.

FIGURE 16.3
The Backup File
Location page



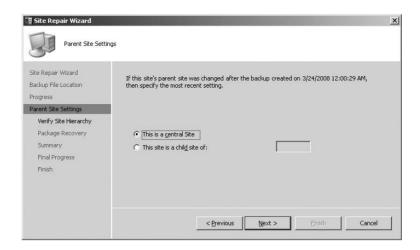
3. On the Progress page, shown in Figure 16.4, watch the steps that the Site Repair Wizard takes to begin the repair process to make sure that they have completed successfully, and click Next.

FIGURE 16.4
The Progress page



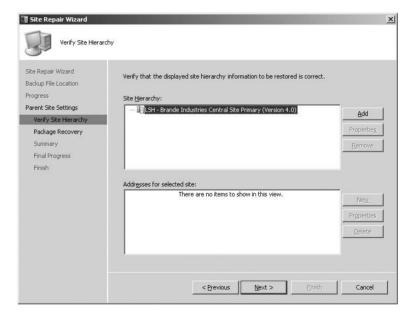
4. On the Parent Site Settings page, shown in Figure 16.5, make sure that a Central Site is selected.

FIGURE 16.5
The Parent Site
Settings page



5. On the Verify Site Hierarchy page, shown in Figure 16.6, you will need to verify that the displayed site hierarchy information to be restored from backup is correct.

FIGURE 16.6The Verify Site Hierarchy page



6. If you have set up a reference site for your central site, or if you have more than one primary site in your hierarchy, you might also see a Reference Connection page at this point. If you do, select a site that was active and accessible to the site you are recovering from the time of the last backup snapshot and the time the Site Repair Wizard was started.

The reference site will be used to recover any objects created at the primary site after that site was last backed up. For example, if there was a collection created at the site to be repaired after it was last backed up, the collection can be recovered from the child reference site selected in Recover Data From Reference Site.

From there, on the Reference Site Data Recovery page, review the steps the Site Repair Wizard takes to recover the reference site data to make sure the process completed successfully and click Next.

Next, on the Object Pad page, enter the approximate number of Collections, Packages, and Advertisements that were created at this site since it was last backed up. This will make sure that future objects that you create after the site is repaired won't have duplicate IDs to those already created. If you don't enter any data in Collections, Packages, and Advertisements, it is based on data recovered from a reference site.

7. On the Package Recovery page, shown in Figure 16.7, you can verify that software distribution source files are accessible to the site server and that the local distribution point is up-to-date. To make sure that the local distribution point is updated with the up-to-date version of the software distribution source files, you can click "Update the distribution point on this site server." If a distribution was not installed on the site server to be repaired, you can skip this step by clicking "Skip package verification."

FIGURE 16.7 The Package Recovery page



- **8.** On the Summary page, shown in Figure 16.8, review the summary of site repair actions that you have selected. If you need to change anything, click Back. Otherwise, click Next to start the repair process. Note that once you click Next here, the repair process will start and you won't be able to go back.
- **9.** On the Final Progress page, shown in Figure 16.9, review the steps that the Site Repair Wizard did to repair the site to make sure they have completed and then click Next.
- **10.** On the Finish page, shown in Figure 16.10, review the information and click Close to finish the site repair process and close the Site Repair Wizard.

FIGURE 16.8
The Summary page

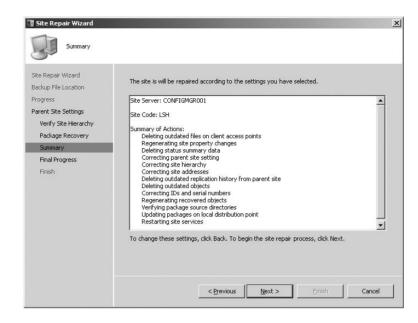
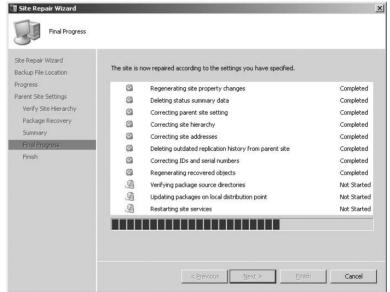


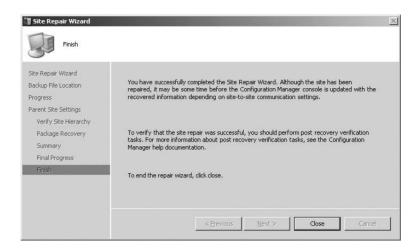
FIGURE 16.9
The Final Progress page



Recovering a Primary Site

Recovering a primary site is almost identical to recovering a central site, except for a few obvious differences in some of the steps. For example, one of these occurs during the Parent Site Settings section of the wizard, Step 4 in the previous procedure, illustrated in Figure 16.5. When restoring a primary site, you will select "This site is a child site of:" and then enter the site code of the site's parent server before you continue.

FIGURE 16.10
The Finish page



Otherwise the Site Repair Wizard will have pretty much the same options as for repairing a central site, depending on the setup of the primary site that you are repairing.

Performing a Site Reset After Recovery

After a site server has been repaired with the Site Repair Wizard, the other roles that the server might have installed will not be reinstalled until you do a Site Reset on the recovered site. This step is required for full recovery of any site system.

- 1. Make sure that any open ConfigMgr consoles are closed.
- 2. On the site that should perform the site reset, click Start ➤ All Programs ➤ Microsoft System Center ➤ Configuration Manager 2007 ➤ ConfigMgr Setup. This will bring up the Configuration Manager Setup Wizard. Click Next to continue.
- **3.** From the Available Setup Options page, shown in Figure 16.11, choose the "Perform site maintenance or reset this Site" option and click Next.
- **4.** On the Site Maintenance page, shown in Figure 16.12, check the "Re-apply default file and registry permissions on this site server" option and click Next.
- 5. You will see a popup like the one shown in Figure 16.13. Click Yes, and then watch as the site reset completes.

Post-Site-Repair Tasks

After you repair a site and the site reset has finished, there are tasks that you should do to make sure that the site you repaired has been properly repaired and is functioning correctly:

- Check site addresses
- Monitor site processes
- Verify site setting configuration

FIGURE 16.11
The Available Setup
Options page



FIGURE 16.12The Site Maintenance page



FIGURE 16.13
The Perform Site Reset?
page



CHECKING SITE ADDRESSES

Follow these steps to check the restored site addresses:

- **1.** In the ConfigMgr console, go to System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ <*site code*> ➤ <*site name*> ➤ Site Settings Addresses.
- Check the results pane and check each address to make sure that it is configured properly for communication with other sites.

MONITOR SITE PROCESSES

Take the following steps to monitor the restored site processes:

- In the Configuration Manager console, navigate to System Center Configuration Manager
 Site Database ➤ System Status ➤ Site Status ➤ <side code> ➤ <site name>.
- 2. Open up the Component Status section and review the Status column to make sure that all of the site components are showing that they are OK. If a site component is not OK, right-click the component, click Show Messages, and then click All to show the status messages for the component so you can diagnose the problem.
- **3.** Open up the Site System Status and check the Status column to make sure that all of the site systems listed are showing that they are OK. If a site system is not OK, right-click the site system's name and click Show Messages, and then click All to bring up the site system status messages so you can diagnose the problem.

CHECK SITE SETTINGS CONFIGURATION

Follow these steps to check the restored site settings:

- **1.** In the Configuration Manager console, go to System Center Configuration Manager ➤ Site Database ➤ *<site code>* ➤ *<site name>* ➤ Site Settings.
- **2.** Review each site setting for your repaired site to make sure all are set up correctly.

The Hierarchy Maintenance Tool (Preinst.exe)

The Hierarchy Maintenance tool (preinst.exe) is a command-line tool that you may need to use to diagnose problems with a site system, help repair a site, shut down site systems, or do other maintenance tasks that, for whatever reason, can't be performed through the ConfigMgr console. This tool must be run locally on a primary or secondary site server computer. Some tasks that preinst.exe does can only be performed on a primary or secondary server.

To use the Hierarchy Maintenance tool, do the following:

- On the Start Menu, click Run, and then enter cmd to open a command prompt window.
- 2. Navigate to the location of preinst.exe, which by default is

<drive ConfigMgr is installed>\SMS\bin\i386\<language code>
(00000409 for English)

- **3.** Once you are there, you can just type **preinst.exe** to get a list of command-line options.
- **4.** Then use preinst.exe with its command-line options, listed in Table 16.3 (adapted from Microsoft documentation), to complete your task.

Hierarchy Maintenance Tool Syntax **TABLE 16.3:**

COMMAND	DESCRIPTION		
/cdupgrade <secondary site code></secondary 	This command is run from a parent site and is used to upgrade a secondary site with installation source files that are present on the secondary site. You can use this command to upgrade a secondary site that failed through the console. Make sure you use the /deljob command before doing this to halt the failed upgrade.		
/deinstall <secondary site code></secondary 	When you use this command on a primary site, it will remove the secondary site you choose from the hierarchy. You can use this command if the deletion of a secondary site failed through the ConfigMgr console.		
/deljob <site code=""></site>	This command is run from the source site and deletes all outbound traffic that is targeted to the site you specify in the command line. This will delete all jobs, or commands, that are targeted to the chosen site.		
/delsite <removed child site code> <parent code="" site=""></parent></removed 	This command, which you run from the parent site, will delete child sites that were not removed successfully previously from the site database of its parent site.		
/dump <i><site code=""></site></i>	This command will write site control images to the root of the folder of the drive that the site is installed on. /dump <site code=""> writes the site control file of only the site specified. /dump will write the site control files for all sites. This image is a binary copy of the site control file, which is stored in the ConfigMgr database. It will contain the sum of the base image and the pending delta images. After you dump a site control file with this tool, the file name will be in the format of sitectrl_<sitecode>.ct0</sitecode></site>		
/stopsite	This command will start a shutdown cycle for the Configuration Manager 2007 Site Component Manager service, which will partially reset the site. When this shutdown cycle is run, some ConfigMgr services on a site server and its remote systems will be stopped. These services are flagged for reinstall, and some passwords will be automatically changed when these services are reinstalled. When the shutdown cycle is started, it will automatically run and skip any computers or components that are not responding. If the Site Component Manager service can't access a remote site system during this process, the components on the remote site system will be reinstalled when the Site Component Manager service is restarted. This will continue until the Site Component Manager succeeds in reinstalling all services that are marked for reinstallation. You can restart the Site Component Manager service using Service Manager just like other Windows services. After you use the /stopsite command to start a shutdown cycle, there is nothing you can do to stop the subsequent reinstall cycles when the Site Component Manager service is restarted.		

TABLE 16.3: Hierarchy Maintenance Tool Syntax (CONTINUED)

COMMAND	DESCRIPTION
/syncchild <i><site< i=""> code></site<></i>	This command, which you run from a parent site, synchronizes a child site with its parent site. This command will simulate a child site attachment so that all components at the current site will be triggered by a site attachment notification, which will update the child site.
/syncparent	This command is run from child sites, and it is used to force all site control images in the site database to simultaneously be sent up to the parent of the current site. This includes sending all the site control images of all child sites stored in the site database of the current site. Use this option if sites are out of synchronization due to time lags or other failures. Because secondary sites don't have a site database, stop and restart the SMS Executive service instead of using the /synchparent command on secondary sites.
/upgrade <secondary site code></secondary 	This command is exactly like /cdupgrade, except it assumes that there are no local setup files on the secondary site and will copy them there before beginning the site upgrade.
/keyforparent	This command is run on sites that you are trying to recover after failure and is used to distribute the new public key to a parent site of the failed site. The /keyforparent command will place the public key of the failed site in the file <site code="">.CT4 at the root of the drive from where the command is run. After the file is made, you will have to manually copy the file to the parent site's hman.box inbox (not in the pubkey folder).</site>
/keyforchild	This command is run on sites that you are trying to recover after failure and is used to distribute the new public key to a child site of the failed site. The /keyforchild command will place the public key of the failed site in the file <site code="">.CT6 at the root of the drive from where the command is run. After the file is made, you will have to manually copy the file to the child site's hman.box inbox (not in the pubkey folder).</site>
/childkeys	This command is run on the recovering site's child sites and is used to distribute public keys from all child sites to the recovering site. The /childkeys command places this and all child site public keys into the file <site code="">.CT6 at the root of the drive from where the command is run. After the file is made, you will have to manually copy the file to the parent site's hman.box inbox (not in the pubkey folder).</site>
/parentkeys	This command is run on the recovering site's parent site and is used to distribute public keys from all parent sites to the recovering site. The /parentkeys command places this and all parent site public keys into the file <site code="">.CT7 root of the drive from where the command is run. After the file is made, you will have to manually copy the file to the child site's hman.box inbox (not in the pubkey folder).</site>

Real World Scenario

MONDAY MORNING SURPRISE

Brande Industries' central office has had a server hardware problem that caused the server to go offline overnight. The ConfigMgr Admin comes in the next morning to find this condition and, after replacing the defective part, discovers that the central site has been corrupted and is not working properly.

The Admin starts the site recovery process and finds that the backup on the local server is also corrupted, causing him to check his archive of offsite backups to find a good backup snapshot. After going through a week's worth of backups, the Admin is finally able to find a snapshot that was not corrupted, restore the site to working condition, and then get the central caught up with info from its child primary sites.

The Bottom Line

Configure backups for Configuration Manager Sites Backing up Configuration Manager sites can be automated by scheduling the Backup ConfigMgr Site Server maintenance task. When the Configuration Manager backup service (SMS_SITE_BACKUP) starts, it uses instructions in the backup control file, located at

[ConfigMgr Install Location]\Inboxes\smsbkup.box\smsbkup.ctl

Master It Recovering Configuration Manager sites are only supported with site backups from what source?

Restore Configuration Manager Sites Recovery of a Configuration Manager site is required if that site is installed with a site code or site server name that has already been used in the hierarchy. Repairing and resynchronizing data is what site recovery is designed for and is required to keep interruption of operations and corruption of data.

Master It What is Site Recovery designed for?

Archive Backup Snapshots to Another Location The first time the Backup ConfigMgr Site Server task runs, it creates a backup snapshot, which can be used to recover a Configuration Manager Site system when it fails. The next time that the backup task runs, it makes a new backup snapshot that will overwrite the one that was made during the last snapshot. This could be a problem if the current backup snapshot becomes corrupt for some reason, as there will not be another backup to restore from.

Master It What script can you use to copy backup snapshots off of the site server to a new location, but is not created when ConfigMgr is installed?

Appendix

The Bottom Line

Chapter 2: Planning a Configuration Manager Infrastructure

Gather deployment intelligence that you will need to plan a Configuration Manager infrastructure for your organization. Deployment intelligence is extremely important in the success of planning your deployment, and people often overlook this step or don't gather enough information to properly plan for what their company might need to get out of the Configuration Manager system.

Master It What are the three parts of deployment intelligence?

Solution Identifying and ranking the current and/or future business needs of your organization is imperative to any successful software implementation:

- ◆ Determine what needs to be accomplished with Configuration Manager.
- Determine what is on the network now and what has been on it in the past.
- Test Configuration Manager in an isolated lab.

Use the deployment intelligence that you have gathered to plan and design a Configuration Manager deployment. After you have gathered your deployment intelligence, you can use all this information to plan your deployment of Configuration Manager.

Master It If you configure Configuration Manager sites with overlapping boundaries, what could happen to the clients assigned to those sites?

Solution The results are unpredictable, and Configuration Manager could end up not being able to manage those clients at all.

Chapter 3: Inoperability with Systems Management Server 2003

Describe the three strategies to move to System Center Configuration Manager 2007 There are three basic paths to get from SMS 2003 to Configuration Manager 2007. As covered in this chapter, it's not always a choice of just one; sometimes you must use a combination of tools within your arsenal. Don't forget that it might not always be a perfectly straight line from Point A to Point C.

Master It A current implementation of SMS 2003 has been running within the enterprise for the past several years. Unfortunately, the Central Primary Site Server does not meet the minimum hardware requirements necessary to run Configuration Manager 2007 R2. Your manager wants to retain all of the work done in SMS 2003 for historical and reporting purposes. Which of the three strategies could be leveraged to migrate to Configuration Manager?

Solution The simple answer is an In-Place Upgrade. The twist to the answer is where you must reach into your bag of tricks and use everything you know about the product and processes. The indirect answer would be to conduct a disaster recovery scenario where you back up your current SMS 2003 implementation but recover it to new hardware that meets the minimum requirements for Configuration Manager 2007 R2. Once SMS 2003 is successfully running on the new hardware, an In-Place Upgrade can take place.

Manage Interoperability Scenarios Within this first step of "Where are you?" an administrator must identify what system requirements are needed in order to install and run Configuration Manager 2007 R2. Although the system requirements for installing Configuration Manager R2 may not seem like they represent the hardware you would want to run your Configuration Manager system on, you should be aware of the hardware and software requirements so that you know which systems in your environment can support it.

Once the minimum requirements are identified, they must be mapped to the current SMS 2003 installation to ensure the appropriate hardware, software, and licenses are in place. This should include documenting the current SMS 2003 infrastructure with a tool such as Microsoft Visio. Microsoft has created a connector for Visio to connect into an SMS 2003 hierarchy and automatically create an infrastructure diagram.

Master It An environment that contains 5,000 machines and is geographically dispersed over 10 states has Microsoft SMS 2003 Service Pack 1 running on Microsoft SQL 2005. The hierarchy is a single Primary Site with nine Secondary Sites at each of the remote locations. What are any potential interoperability scenarios which might exist?

Solution The Microsoft SMS 2003 hierarchy must be on SMS 2003 Service Pack 2 at a minimum as well as Microsoft SQL 2005 Service Pack 1. Additionally, SMS 2003 clients must be at a minimum of Microsoft Windows 2000 Service Pack 4.

Plan the Site Hierarchy Configuration Manager 2007 R2 brings a wealth of new features and functions to enable organizations to have a well-managed enterprise. When addressing the question of "Where do you want to be," these features support business scenarios or business pains such as managing mobile workforces outside of the physical corporate networks, addressing governmental or organizational compliancy, and standardization of operating system configurations. A successful administrator or a successful project will typically address a scenario or set of scenarios and use them as success criteria which Configuration Manager 2007 R2 will address.

Master It An environment that contains 5,000 machines and is geographically dispersed over 10 states has Microsoft SMS 2003 Service Pack 3 running on Microsoft SQL 2005 Service Pack 1. The hierarchy is a single Primary Site with nine Secondary Sites at each of the remote locations. Currently there is a mix of client operating systems from Microsoft

Windows 98 to Microsoft Windows Vista. What might be the plan to get the enterprise managed by Microsoft System Center Configuration Manager 2007 R2?

Solution Because Microsoft Windows 98 exists in the environment, you must decide whether it is truly needed within the business. The first step could be a modified Side-by-Side migration where a Configuration Manager 2007 R2 site is placed as the Central/Parent Site for the current SMS 2003 SP3 site. Clients that meet the system requirements can be upgraded and pushed over to the Configuration Manager 2007 R2 site while the business addresses the viability of Windows 98 in the environment. Once those clients are updated, they can be rolled into the Configuration Manager 2007 R2 environment.

Upgrade from a prior installation of Systems Management Server 2003 Force yourself to produce a project plan in order to address the lasting questions of "How do I get there?" Forcing yourself to write out a project plan makes you think critically of the end-to-end tasks that need to be completed to move from SMS 2003 to Configuration Manager 2007 R2 successfully. Share this plan with peers, your manager, or the Change Review Committee. A project plan is always better when many sets of eyes have looked it over.

The next step of the process is to execute your well-defined project of migrating from SMS 2003 to System Center Configuration Manager 2007 R2. If you've followed the guidelines thus far, the execution should be the easiest part. Use one of the supported methods to upgrade.

Last, and most important, is to celebrate your successes. As in the previous step, once you've identified what went well from the entire project, celebrate the success of your project and enjoy all the rich features of System Center Configuration Manager 2007 R2!

Master It An environment that contains 5,000 machines and is geographically dispersed over 10 states has Microsoft SMS 2003 Service Pack 1 running on Microsoft SQL 2005. The hierarchy is a single Primary Site with nine Secondary Sites at each of the remote locations. Each remote office has approximately 5 to 25 clients, which are the remote sales force. Which new Configuration Manager 2007 R2 roles might be taken into consideration upon a successful upgrade?

Solution Because this is a remote sales force, it is important to consider the Internet-Based Client Management capabilities. A Configuration Manager 2007 R2 role that may potentially be enabled at each location is a Branch Distribution Point. Through the combined capabilities of Internet-Based Client Management and Branch Distribution Points, there could be the potential to nine servers from the remote offices.

Chapter 4: Installation and Site Role Configuration

System Center Configuration Manager 2007 is built upon the collective learning of Systems Management Server that Microsoft has built on over the past 14 years. The foundational concepts have not varied drastically since SMS 1.0. These attributes are site types, site relationships, and various site roles.

Identify the different types of Configuration Manager 2007 sites. When discussing the Configuration Manager 2007 site types, they fall into three general types. Each one of these site types has strengths and weaknesses depending on the business scenario that is being

addressed. When architecting a Configuration Manager solution, leverage all the available features within these types.

Master It List and describe the attributes of the three different types of Configuration Manager site types.

Solution *Central site*: This is the topmost primary site that contains the central SQL repository of all the clients in the hierarchy. It can support up to approximately 200,000 clients and all their associated data.

Primary site: This is a Configuration Manager 2007 site that has a SQL 2005 Service Pack 1 database to store its client data in. Configuration Manager 2007 clients will be assigned only to a primary site Server type.

Secondary site: This is a Configuration Manager 2007 site without a SQL database. Since there is not a database, clients use this site type as a resource for client activities. Depending on the secondary site roles, clients may report client inventories, request Configuration Manager policies, or receive software installation files and instructions.

Define Configuration Manager 2007 site relationships. When multiple Configuration Manager 2007 sites exist within an organization, they have the ability to interact with one another. This interaction is known as *site relationships*. There are two distinct relationships between Configuration Manager sites.

Master It List and describe the two types of relationships of Configuration Manager sites.

Solution *Parent site*: This is a primary site that has either a primary or secondary site attached to it and is sending data up to it. The purpose is threefold and can be a combination of these three general reasons:

- Administrative provisioning and control
- Scale
- Protecting the WAN through site sender settings

Child site: This is a site server, primary or secondary, that is attached to a primary site server and passes its data to be stored in the database. If the child site is a primary site server, all data resides locally as well as a portion being forwarded to the parent site.

Configure Configuration Manager 2007 site relationships. Once the architected solution has been drafted, the implementation of the Configuration Manager 2007 sites must be configured. To have visibility of all the enterprise assets, a site hierarchy must be established by leveraging site relationships.

Master It Create the central/primary site, and leverage a second server (physical or virtual) to install a secondary site server.

Solution Take the following steps:

 Managing the second server, add the primary site server machine account in the second server's Local Administrators group.

- 2. Open the Configuration Manager 2007 console, and expand the Site Management node.
- 3. Right-click the CEN Site node, and select New Secondary Site.
- 4. In the Secondary Site Creation Wizard, click Next.
- **5.** Type **SEC** in the Site Code area.
- **6.** Type a site name description of **Test Secondary Site**, and click Next.
- 7. Type the second server's NetBIOS name in the Site Server Name field.
- Type the installation directory (usually d:\Program Files\ConfgMgr2007) in the Installation Directory field, and click Next.
- Leaving the default radio button of Copy Installation Source Files Over The Network From The Parent Site Server, click Next.
- 10. Leaving the default radio button of Yes. Create a New Address, and click Next.
- **11.** Click Next again for the next two wizard pages.
- **12.** Review the Summary Details page, and select Next and then Close.

Enable and configure the essential Configuration Manager 2007 site system roles. When setting up a primary site server for a System Center Configuration Manager site, there are essential site system roles to enable immediately, while others are optional. The first and foremost is that there is at least one primary site server in the hierarchy; this is the first Configuration Manager 2007 server that is installed. Additional servers may or may not be added depending on the scale and availability needed.

There are essential site roles needed by Configuration Manager to perform the most basic of tasks such as client installation and inventories. Additionally, there are optional roles to install and configure in order to perform advanced functionalities. Not all site roles need to be installed and configured, and each role doesn't need its own server (a common misconception).

Master It Enable and configure the following site roles:

- Distribution point
- Management point
- Reporting point
- Server locator point

Solution Take the following steps to configure a distribution point:

- 1. Open the Configuration Manager 2007 console.
- 2. Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.
- Right-click the primary site server name, and select New Roles.
- 4. In the New Site Role Wizard, click Next.
- **5.** Under Available Roles, select the Distribution Point box.

- Click Next.
- 7. Review the Summary Details page, and click Next.
- Select Close.

Take the following steps to configure a management point:

- **1.** Open the Configuration Manager 2007 console.
- **2.** Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.
- Right-click the primary site server name, and select New Roles.
- 4. On the New Site Role Wizard, click Next.
- 5. Under Available Roles, select the Management Point box, and click Next.
- Review the Summary Details, and click Next and then Close.
- Review the rsetup.log file on the primary site server logs directory for "Installation was successful."

Take the following steps to configure a reporting point:

- **1.** Open the Configuration Manager 2007 console.
- 2. Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.
- 3. Right-click the primary site server name, and select New Roles.
- 4. In the New Site Role Wizard, click Next.
- 5. Under Available Roles, select the Reporting Point box, and click Next.
- Review the Summary Details page, and click Next and then Close.
- Review the rsetup.log file on the primary site server logs directory for "Return 0" and "Finished."
- 8. Review the SMSReportingInstall.log file for "Installation of Reporting Point Complete."

Take the following steps to configure a server locator point:

- **1.** Open the Configuration Manager 2007 console.
- Expand the Site Management node, and choose CEN ➤ Site Settings ➤ Site Systems.
- Right-click the primary site server name, and select New Roles.
- 4. On the New Site Role Wizard, click Next.
- 5. Under Available Roles, select the Server Locator Point box, and click Next.
- **6.** Review the Summary Details, and click Next and then Close.
- Review the SLPMSI.log on the primary site Server logs directory for "Product: SMS Server Locator Point – Configuration completed successfully."

Chapter 5: Client Installation

Configure Client Push Installation When configuring the Client Push Installation method, you need to make sure the required settings are in place. You must define boundaries, configure Active Directory extensions, configure the Client Push Installation properties, and run discovery methods to find the computer.

Master It You need to set up Configuration Manager to install the client software automatically on any client it discovers.

Solution First you need to create the Client Push Installation account:

- 1. Log on to the domain controller.
- 2. Open Active Directory Users and Computers.
- 3. Right-click the OU where you want to create the user account and select New ➤ User.
- 4. Name the account ClientPushInstaller.
- Enter the password for the account and select Password Never Expires. Then click Next and Finish.
- **6.** Right-click the account and select Add To Group.
- 7. Type Domain Admins and click OK.
- **8.** Click OK to acknowledge the account was added.

Next configure the boundaries:

- Open the console and navigate to Systems Management Server ➤ SiteServerName ➤ Site
 Management ➤ SiteCode ➤ Site Settings ➤ Boundaries.
- 2. Right-click Boundaries and select New Boundary.
- **3.** Make sure IP Subnet is selected from the Type: drop-down.
- **4.** Enter your IP network address in the Network field.
- **5.** Enter the subnet mask for your network in the Subnet Mask field.
- **6.** Make sure Fast (LAN) is selected under Network Connection and click OK.

Configure the Client Push Installation method as follows:

- 1. Select the Client Installation Methods node.
- 2. Right-click Client Push Installation from the details pane and select Properties.
- **3.** In the Client Push Installation Properties dialog, select the Accounts tab.
- Click the New button.
- 5. In the User Name text field, enter the name of your Client Push Installation account in the form domain\account.

- **6.** Enter the password in the password fields, and then click OK.
- Select the Client tab.
- 8. In the Installation Properties text box, make sure the SMSSiteCode entry is included, and then click in the text box so that the cursor is at the end of the line.
- Enter the following: properties: CCMENABLELOGGING=TRUE CCMLOGLEVEL =0 CCMMAXHISTORY=3 SMSCACHESIZE=1024.
- 10. Click OK.

Next, configure the discovery methods:

- 1. Select the Discovery Methods node.
- Right-click the Active Directory System Discovery tool in the details pane and select Properties.
- **3.** Select the checkbox for Enable Active Directory System Discovery.
- 4. Click the New button.
- 5. Leave the default selections for Local Domain and Recursive selected and click OK.
- 6. Leave the domain selected and click OK.
- Select the Polling Schedule tab.
- 8. Leave the daily schedule as the default, and select Run Discovery As Soon As Possible.
- **9.** Select the Active Directory Attribute tab.
- 10. Click the New button.
- **11.** Enter **machineRole** in the Attribute Name field and click OK.
- 12. Click OK.

Verify the discovery, as follows:

- Navigate to Systems Management Server ➤ SiteServerName ➤ Computer Management
 Collections ➤ All Systems.
- 2. Right-click All Systems and select Update Collection Membership.
- Right-click All Systems and select F5.
- Verify that the computer systems appear in the details pane.

And finally, push the client:

- In the All Systems collection, right-click your domain controller and select Install Client.
- 2. When the Client Push Installation Wizard appears, click Next.
- 3. Select the Include Domain Controllers check box.

- 4. Clear the Include Only Client Assigned To This Site check box, and then click Next.
- 5. Review the options and click Finish.
- **6.** On the domain controller, open Task Manager and select the Processes tab.
- 7. Verify that the ccmsetup.exe program is running.
- **8.** When ccmsetup.exe ends and CcmExec.exe starts, open Windows Explorer and Navigate to c:\windows\system32\ccm\logs
- **9.** Verify that log files exist.
- 10. Open Control Panel and Select Systems Management.
- **11.** Click the Advanced tab and verify that the site code is 001 and the cache allocation is set to 1024.

Configure Logon Script Installation When a logon script is used, the command line used to install the client needs to be included in the logon script, or a new logon script that uses the command should be created.

Master It The client needs to be installed on all of the systems within the domain. You want to roll out the client automatically while the end user is logging onto their systems, so you want to configure a logon script so that every machine will get the client when the machine is logged into the network.

Solution Configure the login script for the user within the Active Directory Users and Computers using this command:

CCMSetup /mp:Z28MP01 SMSSiteCode=Z28 FSP=Z28FSP01

It specifies the following:

- The management point of Z28MP01 as the server in which to download the installation files.
- Automatic assignment of the SiteCode of Z28.
- ◆ The fallback status point of Z28FSP01.

Manually Install the Client Installing the client manually is also supported. An administrator needs to install the client on every machine where the client will be used.

Master It The client needs to be installed on all of the systems within the domain. You want to control the roll-out of the client, so you do not want to enable the ability for automatic installation, but you do want to use the push installation method so that you can control the installation from the console.

Solution Take the following steps:

From the client, browse to \\ConfigMgrSRV\SMS\Client Folder, where ConfigMgrSRV is your Configuration Manager server.

2. Run the following command line:

CCMSetup.exe [Ccmsetup properties][client.msi setup properties]

For example, this command line:

CCMSetup /mp:Z28MP01 SMSSiteCode=Z28

has the following effect:

- Specifies the management point of Z28MP01 as the server in which to download the installation files.
- Automatic assignment of the SiteCode of Z28.

Chapter 6: Software Distribution

Plan for software distribution. Microsoft greatly expanded Configuration Manager's granularity of configuration for software distribution. It now gives an administrator a lot more options for planning and deploying software that meets their business needs.

Master It A branch distribution point (BDP) is designed for small branch offices that have a minimal amount of resources and/or bandwidth at their location. They function a lot like standard distribution points but provide greater control over the scheduling and throttling of network traffic by using BITS. BDPs use BITS like a standard distribution point, but do they require IIS to work?

Solution No. Branch distribution points leverage a BITS client that is installed when the Configuration Manager client is installed.

Create and manage packages. Packages are what Configuration Manager uses to send software to clients and are the core of the software distribution feature. Packages can be anything from a full-fledged software install such as Microsoft Office 2007 to a script to change the administrator password on workstations to just a shortcut that you want copied to your user's desktop.

Master It How do you get to the Packages node in the Configuration Manager console?

Solution Go to System Center Configuration Manager ➤ Site Database ➤ Computer Management ➤ Software Distribution. There you will find the Packages and Advertisement nodes.

Create and manage programs. Although a package has all the source files or information needed to be sent to client computers, it is the program that actually tells the client what to do with the package files when it is time to run them. Each package should have at least one program and should contain all references to install files, scripts, or command-line switches that are needed to run the program.

Master It What is the default setting for the maximum allowed run time of a program?

Solution 120 minutes.

Create and manage distribution points. Distribution points are site servers or shares that store files for packages so they can be used to be run on client computers. These files can either be run from the distribution point over the network or run locally after the files have been downloaded to the client's cache.

Master It What setting has to be enabled on a distribution point to allow the use of BITS network throttling?

Solution The Allow Clients To Transfer Content From This Distribution Point Using BITS, HTTP, And HTTPS setting.

Create and manage collections. Collections are an essential part of the software distribution process because they represent groups of resources that are used as targets for software deployments. Collection membership either can be by direct assignment or can be query based. With direct membership, you must manually add the resources that belong to that collection and also manually update that collection as resources are added or deleted. Query-based membership is dynamic, so you do not have to manually manage the resources in the collection, and it is updated automatically on a specific schedule.

Master It On what page of the New Collection Wizard do you configure collection membership?

Solution The Membership Rules page.

Create and manage advertisements. To get a program to run on a client, you must set up an advertisement that sends the package and program information to a collection of clients that you want to run the program.

Master It What information is sent to clients in an advertisement?

Solution

- ◆ The program that is to run on the client
- The collection that is to get that program
- When the program will be available to clients, for how long, and whether the program will be mandatory

Monitor software deployments. The results from software distribution reports are made from direct SQL queries on the Configuration Manager database. They are snapshots of data taken from the time that the report is run.

Master It Which is the best report for viewing the status of an advertisement?

Solution The Status of a Specific Advertisement report.

Chapter 7: Software Updates

Plan to Use Software Updates You can use the same method of "deployment intelligence" that was used in Chapter 2, to gather information for planning to implement Software Updates. This will be very helpful in making sure that you get the most out of the Software Updates feature for your organization.

Master It What is the first step in gathering "deployment intelligence" for planning to implement Software Updates?

Solution Determine what needs to be accomplished with Software Updates.

Configure Software Updates Before you can utilize Software Updates in your environment, the various components of this feature need to be set up and configured.

Master It What is the very first thing you have to install before you can use Software **Updates?**

Solution Windows Server Update Services (WSUS) 3.0. Either the full install or the WSUS Admin console, depending on what you are setting up.

Use the Software Updates Feature to Manage Software Updates The hardest thing to do in SMS 2003 relating to patch management was to programmatically prioritize software updates that are critical so they can be deployed with a higher priority than other updates.

Master It What does Configuration Manager provide that can help with prioritizing software updates?

Solution Configuration Manager now includes the severity of all of the updates that are synchronized in to the Configuration Manager database. With that data you can sort updates by that category and create search folders and update lists based on their severity level so that you can use them as a source for your software update components.

Chapter 8: Operating System Deployment

Specify a Network Access account. The Network Access account is the account Configuration Manager will use to access the system while running WinPE.

Master It How do you specify the Network Access account?

Solution Open the Configuration Manager console, and expand Site Database ➤ Site Management ➤ Site ➤ Site Settings ➤ Client Agents. Right-click the Computer Client Agent, and select Properties. Set the Network Access Account setting to the account you created, and click OK.

Set up a PXE service point. A PXE service point is used by Configuration Manager to begin the operating system deployment process. The PXE service point responds to Configuration Manager clients making PXE boot requests.

Master It How do you set up a PXE service point?

Solution Open the Configuration Manager 2007 console, expand Site Management ➤ Site ➤ Site Settings ➤ Site Systems, select the server that will be the PXE service point, and then right-click the server. Select New Roles, click Next on the General tab, and then select PXE Service Point. Click Next, and then click Yes in the dialog box informing you that the PXE point must have ports opened on the firewall. Then specify whether the computers will require a password to boot to the PXE server. Select the default configurations for the database. Click Next on the Summary page and then Close on the Completed page.

Update the driver catalog package. The driver catalog will allow you to add drivers to the already created packages and images you have within your organization so you are not constantly re-creating your images when you get a new machine in your environment.

Master It How do you update the driver catalog package?

Solution Expand the Drivers node located under Site Database ➤ Computer Management ➤ Operating System Deployment. Right-click the Drivers node, and select Import. Browse to the network location of the drivers you want to import, and then specify which package and boot images you want to import the specific drivers into.

Chapter 9: Asset Intelligence

Enable Asset Intelligence. If you installed Configuration Manager from scratch, you will find that Asset Intelligence is not enabled by default. Depending on the data that you want information on, you will have to edit the Configuration Manager MOF files and make sure that certain client agents are enabled.

Master It What are the classes in the sms_def.mof file that you have to enable to use Asset Intelligence?

Solution You need to enable the following classes in sms_def.mof to use Asset Intelligence:

- SMS SystemConsoleUsage
- SMS_SystemConsoleUser
- SMS_InstalledSoftware
- ◆ SMS InstalledSoftwareMS
- SMS_AutoStartSoftware
- SMS_BrowserHelperObject
- SoftwareLicensingService
- SoftwareLicensingProduct

Enable Client Access License tracking. There are new CAL reports that have been added to the existing License Ledger reports. These reports complete the ability to compare license usage with Microsoft License Statements.

To be able to use those reports, however, you will have to edit the singleton class CCM_CALTrackConfig in the configuration.mof file. That section of the file contains several variables controlling the way that CAL data is collected.

Master It What does the CALCollectionTimeWindow parameter in the configuration .mof file set?

Solution The CALCollectionTimeWindow parameter controls how often CAL licensing can be reassigned. The current Microsoft licensing model allows for CALs to be reassigned every 90 days, so this value shouldn't be modified. If Microsoft changes its licensing model later, you can adjust this value according to the new value to any number from 1 to 365.

Configure the Asset Intelligence Synchronization Point. The Asset Intelligence Synchronization Point is used to connect to System Center Online to synchronize Asset Intelligence catalog information and get periodic updates.

Master It What are the two things that are required in order to use an Asset Intelligence synchronization point?

Solution

- ◆ A Software Assurance account with Microsoft
- ◆ A valid System Center Online authentication certificate

Chapter 10: Inventory and Software Metering

Configure and manage Software Inventory Even though Software Inventory hasn't changed much in Configuration Manager 2007, it is still a very effective tool in the battle of keeping track of what software is on your network.

Master It Eventually you might need to add to the files and file types that are part of the inventory collection in the software inventory of your hierarchy. Where would you go to do that?

Solution Take the following steps:

- In the Configuration Manager console, select System Center Configuration Manager ➤ Site Database ➤ Site Management ➤ site code ➤ site name ➤ Site Settings ➤ Client Agents.
- **2.** In the left pane, right-click Software Inventory Client Agent, and then click Properties.
- **3.** Then click the Inventory tab.

4. Click the New button, and then configure the options for the file that you want to add.

How to configure and manage Hardware Inventory Hardware Inventory provides a wealth of information on the hardware resources in your organization. That information is vital when planning for things such as updating standard business software or upgrading the standard operating system your organization uses. If the standard hardware inventory collected is not enough for your needs, then you have many options to extend hardware inventory to get that vital information.

Master It What part of Hardware Inventory is contained in the sms_def.mof file?

Solution The sms_def.mof file defines the reporting classes used by the Hardware Inventory Client Agent to specify whether specific client data class information is reported.

How to configure and manage Software Metering Keeping track of software that is installed and actually being used is a large part of being able to manage software licenses effectively. With Software Metering in Configuration Manager paired with Software Inventory, you can get detailed information on just what software is out there and who is or is not using it. This goes a long way to help keep your software licensing in compliance.

Master It How long do you have to wait, at the very least, after you configure Software Metering before you can expect to see any data returned?

Solution 12 hours. Software Metering Data Summarization runs daily by default and will run only against data that is at least 12 hours old. This is required for all software metering reports to produce any meaningful data.

Chapter 11: Reporting

Set Up Reporting Point Roles Setting up the Reporting Point role within Configuration Manager allows not only administrators but everyone the ability to view reports in some fashion either via a CSV file or a direct link within the Web Reporting tool.

Master It What is the procedure to enable Reporting with Configuration Manager?

Solution Open the Configuration Manager 2007 console, expand the Site Management node, expand the Site node, expand the Site Settings node, expand the Site Systems node, right-click on the Primary Site Server name, select New Roles, and add the Reporting node to the server.

Create and Manage Reports Creating rich reports will provide you with a single place to get information about your Configuration Manager hierarchy and help you provide information about your environment in a few simple clicks.

Master It What are the steps to importing a report?

Solution Right-click on the Reports node and select Import Objects. Follow the wizard and import your new reports into your Configuration Manager console.

Create and Manage Security on a Single Report Creating rich security for reports will provide you with a great resource to limit which department or individuals can or cannot view individual reports.

Master It What are the steps to securing a report?

Solution Right-click on the individual report you need to modify security and choose Properties. Click on the Security tab and then click on the Star (New) under the Instance security right section. This will open the Object Instance Security Right Properties dialog box. Type in the username (for example, domain\user) in the dialog box. Assign the rights accordingly. You have the option to Delete, Modify, and Read. To allow a user to view a report, they need at least Read access on the report. Click OK. Click OK on the Report Properties Security tab.

Create and Manage Dashboards Creating dashboards is a great place to get access to a lot of different data on one single pane.

Master It Create a custom dashboard that contains two reports.

Solution Right-click on the Dashboard node and select the reports you want to add to your single pane view.

Chapter 12: Desired Configuration Management

Enabling the DCM Agent Until the DCM agent is enabled for your Configuration Manager clients, your clients will not evaluate any of the configuration baselines. This is the first step in using DCM to validate client settings.

Master It Enable the DCM agent for the Configuration Manager clients.

Solution In the Configuration Manager console, under the Client Agents node, open the Desired Configuration Manager client agent and select the box next to "Enable desired configuration management on computer" and then click OK.

Creating Configuration Items Configuration items are the pieces of the puzzle that make up the picture called a configuration baseline. There are a number of different configuration item types in Configuration Manager, and depending on the type you choose to create, you are presented with certain options when assembling your configuration item. The steps to create configuration items were covered in the first part of this chapter, which included several examples on how to create the different types of configuration items.

Master It Create a configuration item for an application that checks a registry string value.

Solution In the Configuration Manager console under the DCM node, make sure you have the Configuration Items folder selected and right-click it. Select New and then Application Configuration Item. In the wizard, enter the following settings:

1. On the General tab, enter

Name: Application name and value description here

Description: Configuration item for ...

Categories: Add categories here

2. On the Objects tab, click New Registry Key from the menu and set the following:

Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\ . . .

Is this registry key associated with a 64-bit application: No

Report a noncompliance event when this instance count fails: Yes/Checked

Instance operator: Greater than

Values: 0

Severity: Warning

- 3. On the Settings tab, click New Registry from the menu.
- 4. On the General tab of the new registry validation, enter

Display name: Friendly name here

Description: Description of what you are checking for here

Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE \ . . .

Value name: Registry keys value name here

Is this registry key associated with a 64-bit application: No

- **5.** On the Validation tab of the new registry validation, set the Data Type to String.
- **6.** Click New on the menu in the details pane and, in the Configure Validation window that appears, make these settings:

Name: Friendly name here

Description: Description of the value you are going to check for here

Operator: Equals or other operator

Value: Value to check the registry key for here

Severity: Warning

7. Click OK to return to the Validation tab of the new registry validation and set the following:

Is this registry key associated with a 64-bit application: No

Report a noncompliance event when this instance count fails: Yes/Checked

Instance operator: Greater than

Values: 0

Severity: Warning

- **8.** Click OK to save your changes to the Settings tab and move on.
- On the Detection Method tab, select the radio button Always Assume Application Is Installed.
- On the Applicability tab, make sure the All Windows Platforms radio button is selected.

Assemble Configuration Baseline This is where you take one or more of the CIs and put them together into a package that the Configuration Manager client downloads and at the scheduled time validates by checking the CIs against the computer. The Configuration Manager client then reports the outcome of those checks back to Configuration Manager where you can then run reports to see if your clients are within the specified configuration or not. These steps were covered in the last section of the chapter.

Master It Assemble a configuration baseline with one or more configuration items you have created.

Solution Follow these steps:

- In the Configuration Manager console under the DCM node, select the Configuration Baseline folder and right-click it; from the context menu, choose New Configuration Baseline.
- The first tab in the New Configuration Baseline Wizard is the Identification tab. Enter an appropriate name for this baseline and a description, and select or create any categories necessary.
- 3. Click the Next button to move to the next tab.
- 4. In the Set Configuration Baseline Rules tab, select the appropriate rule type for the baseline by clicking the hyperlinked word in the rule. This opens another window with all the CIs listed, and you can choose which CIs to add by selecting the check box next to an item's name. After you have selected one or more CIs to add to the rule, click OK to return to the Configuration Baseline Wizard, and then click Next.
- 5. In the Summary tab, you can see all the values and CIs you have entered into the base-line. Clicking the Next button will create the configuration baseline and take you to the final tab in the wizard. Click the Close button, and the baseline creation will be completed.

Chapter 13: Mobile Device Management

Enable a mobile device management point. Setting up a mobile device management point within Configuration Manager gives administrators the ability to manage mobile devices within the Configuration Manager 2007 site.

Master It How do you enable a mobile device management point?

Solution Open the Configuration Manager 2007 console, expand the Site Management node, expand the Site node, expand the Site Settings node, expand the Site Systems node, select the mobile management point server name, right-click ConfigMgr Management Point under Roles, choose Properties, and select the Allow Devices To Use This Management box.

Verify the health of mobile clients. Configuration Manager 2007 has some prebuilt reports to help verify the health of mobile device clients.

Master It View the health status of mobile devices using reports.

Solution Use any of the following reports to verify your mobile device client's health. To view the reports, open the Configuration Manager administrator console, expand the site database, expand the Computer Management node, expand the Reporting node, and expand Reports. Browse for any of the following reports:

- Device Client Agent Deployment Failure Report
- Device Client Agent Deployment Status Details
- Device Client Agent Deployment Success Report
- Device Client Agent Health Summary
- ◆ Device Client in Healthy Condition
- Device Client in Unhealthy Condition Due to Certificate Issues
- ◆ Device Client in Unhealthy Condition Due to Communication Issues
- ◆ Device Client in Unhealthy Condition Due to Local Client Issues

Chapter 14: Network Access Protection

Identify the components that make up NAP and their roles. NAP as a technology has many different parts associated with it, so understanding the terminology and how the various parts interact is critical to understanding and planning for a successful NAP deployment.

Master It What is a system health agent (SHA), and how does this relate to Configuration Manager 2007?

What is a statement of health (SoH)?

What is a system health validator (SHV), and how does this relate to Configuration Manager 2007?

Solution A system health agent is a plug-in that is installed on the desktop of your NAP-capable computers and is responsible for reporting specific health information to the NAP agent service. Configuration Manager 2007 has its own SHA that reports and evaluates the patch state of the machine.

The statement of health contains the posture information of a machine and is sent to the NPS for evaluation at network connect time.

A system health validator is a plug-in that is installed on the NPS and is responsible for doing the health evaluation of the data sent in the SoH by the SHA. Configuration Manager 2007 has its own SHV that plugs into NPS and does patch evaluation for machines connecting to the network.

Integrate your choice of the NAP enforcement methods with your current Configuration Manager 2007 deployment. Each of the four enforcement methods discussed in this chapter has a unique way of handling network access as well as of quarantining of machines that become noncompliant. Once you understand the impact of these access and quarantine methods, you will then be ready to start integrating NAP into your Configuration Manager 2007 environment.

Master It How does NAP quarantine noncompliant machines in DHCP NAP?

In VPN NAP?

In 802.1x (wired or wireless) NAP?

In IPsec NAP?

Solution In DHCP NAP, the DHCP server will issue noncompliant machines an IP address but no default gateway. Then, NPS will tell the NAP service to modify the route table on the host so that the machine can communicate only with the remediation servers that you have defined. In the case of Configuration Manager 2007, these are your distribution points.

In VPN NAP, the NPS will send down a set of IP filters to the VPN server that will then be applied to that machine's VPNs session, thereby restricting where the client can go on the network. In the case of Configuration Manager 2007, these are your distribution points.

In 802.1x NAP, there are two options for quarantining noncompliant machines. The first is to create VLANs on your network and then configure NPS to send VLAN tag information to your switch or WAP to put noncompliant machines into a predefined VLAN that you created. The second method is to configure NPS to send down port ACL information to the switch or WAP, which will tell the device what IP address, protocols, and ports that machine can access.

In IPsec NAP, quarantining is done by the NAP service being notified that the machine is noncompliant and by having the NAP service immediately delete the health certificate from the machine store for that machine while at the same time also tearing down all active security associations that the machine may have with other machines on the network.

Deploy NAP with Configuration Manager 2007 in a phased approach to minimize your risk. Technologies such as NAP and Configuration Manager 2007 require careful planning and thought around the impact of quarantining machines and then autoremediating them. In some cases, network redesign work may be required for those deployments that are larger and more complex. Having the ability to introduce NAP into your Configuration Manager environment is very beneficial in helping you minimize the impact on the users of your network.

Give a brief description of each of these phases in your answers.

Master It Name the three phases of a successful NAP deployment and one benefit of each phase.

Solution Phase 1 is reporting mode, which offers you the following benefits:

- The ability to "take inventory" of the posture of machines on your network as they relate to patch level for Configuration Manager 2007 specifically
- The ability to log critical posture information about machines on your network without doing any kind of quarantining

Phase 2 is deferred enforcement and offers you the following benefits:

- The ability to warn your users that you will take away their network access at a date and time defined by the administrator, which then allows the users to take action themselves to make their machines compliant with your patch policies
- The ability to bring your compliance rates up without you having to deploy any additional servers or quarantining any machines

Phase 3 is full enforcement and offers you the following benefits:

- By quarantining noncompliant machines, you are raising the health level and security of your network.
- By enabling automatic remediation, you are getting the benefits of the first point plus the reduction of help desk calls by having infrastructure in place that allows your machines to remediate themselves without the user taking any action.

Chapter 15: Troubleshooting

Create a basic maintenance plan. Setting up a basic maintenance plan is a vital step to ensure the proper health of your Configuration Manager 2007 hierarchy.

Master It How do you create a basic maintenance plan?

Solution Develop a plan, similar to the guidelines discussed earlier in this chapter. Review and modify the plan on a biannually basis, and update it throughout the year to ensure nothing gets overlooked and the documentation is up-to-date with the current design of the Configuration Manager site.

View log files using SMS Trace. Although using SMS Trace to view log files is not a requirement for viewing log files, it is highly recommended because SMS Trace constantly monitors the opened file for updates.

Master It Using SMS Trace to view log files.

Solution Download and install Configuration Manager 2007 from Microsoft's website. Once it is installed, click Start ➤ Programs ➤ Configuration Manager Toolkit. Within the Toolkit program group, click Trace32.

Then click File, and open and browse to the log file you want to review and open.

View client status report information. One of the advances in Configuration Manager 2007 R2 is the release of client status reporting. Once the feature has been successfully installed and configured, it contains some reports that will help administrators develop a healthy Configuration Manager environment.

Master It View client status reporting reports from the Configuration Manager 2007 console.

Solution Open the Configuration Manager 2007 console. Expand Site Database ➤ Computer Management ➤ Reporting ➤ Reports. Once you open the Reports node, you will be presented with all the reports within your site. Using the built-in filtering tool, type **Client Status** in the Look For text box, and click Find Now.

Chapter 16: Disaster Recovery

Configure backups for Configuration Manager Sites Backing up Configuration Manager sites can be automated by scheduling the Backup ConfigMgr Site Server maintenance task. When the Configuration Manager backup service (SMS_SITE_BACKUP) starts, it uses instructions in the backup control file, located at

[ConfigMgr Install Location]\Inboxes\smsbkup.box\smsbkup.ctl

Master It Recovering Configuration Manager sites are only supported with site backups from what source?

Solution Backups that are created by the Backup ConfigMgr Site Server maintenance task.

Restore Configuration Manager Sites Recovery of a Configuration Manager site is required if that site is installed with a site code or site server name that has already been used in the hierarchy. Repairing and resynchronizing data is what site recovery is designed for and is required to keep interruption of operations and corruption of data.

Master It What is Site Recovery designed for?

Solution Repairing and resynchronizing ConfigMgr data.

Archive Backup Snapshots to Another Location The first time the Backup ConfigMgr Site Server task runs, it creates a backup snapshot, which can be used to recover a Configuration Manager Site system when it fails. The next time that the backup task runs, it makes a new backup snapshot that will overwrite the one that was made during the last snapshot. This could be a problem if the current backup snapshot becomes corrupt for some reason, as there will not be another backup to restore from.

Master It What script can you use to copy backup snapshots off of the site server to a new location, but is not created when ConfigMgr is installed?

Solution AfterBackup.bat

Index

Note to the Reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

A	Add Operating System Image Wizard,
access control lists (ACLs), 494–495	322–323, 322–323
Access Distribution Folder Through Common	Add Software Updates window, 451,
Configuration Manager Package Share	451
option, 191, 292	Add the Software Update Point Role to an
accounts	Existing Server option, 269
client push installation, 143–145 , 144–145	Additional Requirements setting, 202
Network Access, 310 , 310–311	Address to Secondary Site page, 87, 88
Accounts tab, 144, 151, 152	addresses, site, 540
ACLs (access control lists), 494–495	Administrator console
actions	Asset Intelligence, 24
client installation, 160	client installation, 156
mobile device clients, 467	dashboards, 423
site servers, 83	mobile devices, 461, 464
software updates, 257	reports, 410–412, 414, 417
Active Directory (AD)	software upgrades, 239
considerations, 34–36	upgrading, 62–63
discovery methods, 145–151 , 146–150	WSUS, 267
management points, 101	Administrator Manually Copies This Package
schema, 34–35 , 52	To Branch Distribution Points option, 193,
server locator points, 112	294
system health validator points, 123	ADPROG setting, 84
Active Settings tab, 115, 116	Advanced page for programs, 203-204, 204
Active Software Update Point Settings page,	Advertised Programs Client Agent, 167
270–271, 270, 272	description, 142
active Software Update Points, 115, 116,	General tab, 167–168 , 168
269–275 , 270–275	Notification tab, 168–169 , <i>169</i> , 173, 175
ActiveSync Service Status report, 467, 467	Advertised Programs window, 475, 475
Activity Management Technology (AMT), 22,	Advertisement report, 407
125	Advertisement Start Time setting, 217
Add Driver To Boot Images page, 345, 346	Advertisement Status reports, 406–407
Add Driver To Packages page, 345, 346	Advertisement Status window, 331, 331

Advertisement Will Expire setting, 217	Allow This Program To Be Installed From The
advertisements	Install Program Task Sequence option,
collections, 181, 182	programs, 204
creating, 214–221 , 215–219, 221	Allow User Targeted Advertisement Requests
images, 322–323 , 322–323	option, 167–168
packages to clients, 465–467, 466, 469–472,	Allow Users To Run The Program
470-473, 477-479, 478-479	Independently Of Assignments option, 220
security, 220	Always Obtain Files From The Source
software distribution, 165, 171 , 173, 217, 406	Directory option, 189, 198
status messages, 512–513	Always Rerun Program option, 218
status reports, 221–222, 223–226	Always Run This Program First option, 204
task sequences	AMT (Activity Management Technology), 22,
bare-metal, 343–344 , <i>343</i>	125
reports, 407	Applicability page
steps, 328–331 , 329–331	configuration items, 445 device drivers, 344, 345
virtual application packages, 233	application CIs, 426–427, 452
Advertisements page, 181, 182	Application Virtualization (App-V), 25 , 135
Advertisements report, 406	packages, 231–233
After Running setting, 200	software distribution, 165
AfterBackup.bat file, 526–527	archiving backups snapshots, 526–527
agents	ASC keyword, 419
client. See client agents	Asset Intelligence (AI), 24, 349
DCM, 428 , 429	catalog, 352–355
AI. See Asset Intelligence (AI)	client access license data, 363–366 , <i>364</i> , <i>366</i>
Allow Clients To Connect Anonymously	enabling, 362–363 , <i>363</i>
option, 213, 460, 461	home page, 356–358 , <i>357</i>
Allow Clients To Fallback To Unprotected	new features, 349–350
Distribution Points option, 220	reports, 358–362 , 404
Allow Clients To Transfer Content From This	requirements, 350–352
Distribution Point Using BITS, HTTP, Or	synchronization points, 355 , 365–366 , <i>366</i>
HTTPS option, 213, 460	validation states, 355–356
Allow Devices To Use This Management Point	Asset Intelligence 1.5 update, 125–127 , 125–127
option, 459, 460	Asset Intelligence Synchronization Point
Allow Display Notifications On Clients option,	Connection Settings page, 366, 366 AssetMetrix technology, 349
300	Assign Configuration Baseline Wizard,
Allow only site server initiated data transfers	454–455, 455
from this site system option, 209, 270	Assignment report, 404
Allow Signed Content from Intranet Microsoft	attended client push installation, 155–157 , <i>156</i>
Update Service Location option, 258	attributes for configuration items, 439–441,
Allow System Restart Outside Maintenance	440–441
Windows option, 218, 255	Attributes tab, 439

Audit report, 407	PXE service points, 331–334 , 332–334
authentication, 484, 487, 496	task sequences, 339–344 , 340–343
automatic methods	baselines, configuration, 425, 431
client installation, 157–159	clients, 454–455 , <i>455</i>
management point queries, 101	configuration items for, 453, 453-454
Automatic Rule Generation feature, 393–395	initial, 449–450
Automatically Download Content When	options, 455
Packages Are Assigned To Branch	rules, 450–453 , <i>451</i>
Distribution Points option, 193, 293	BDP (Branch Distribution Points)
Automatically obtain latest Windows Update	capabilities, 93
Catalog screen, 280, 281	creating, 213–214 , 214
Autorun program, 72–73, 73	software distribution, 164, 170
Availability Management process, 5–6 , 10	Binary Delta replication, 164
Available Setup Options page	BITS. See Background Intelligent Transfer
site reset, 538, 539	Service (BITS)
site servers, 73, 73	BITS tab
Available Software Updates dialog box, 249	Computer Client Agent, 257
	software distribution, 173, 174
В	boot image packages, 316–318, 319
Background Intelligent Transfer Service (BITS)	Boot Image page, 318, 319
Computer Client Agent, 257	boundaries
distribution points, 92, 95	client push installation, 143, 144–145
interrupted downloads, 165	site, 36 , 47–50 , <i>50</i>
mobile devices, 460	Branch Distribution Point on Client System
software distribution, 173, 174	log, 97
Backup ConfigMgr Site Server task, 502, 502,	Branch Distribution Points (BDP)
523–529 , <i>528</i>	capabilities, 93
Backup File Location page, 533–534, 534	creating, 213–214 , 214
Backup Secondary Site Server task, 529	software distribution, 164, 170
Backup Site Server task, 528, 528	Browse Collection dialog box, 216, 216
backups, 524	Browse for Folder dialog box, 533
archiving snapshots, 526–527	Browse Query window, 185, 185
central site, 524–525	build phase in SMS upgrades, 57
copying to other locations, 525–526	1
restoring, 529–532	С
bandwidth considerations	caches
site design, 37–38	clients, 154–155
software distribution, 170	software distribution, 165, 190
bank software, 354	Capacity Management process, 5, 10
bare metal operating system deployment,	Capacity Planner, 14
331	capture image, 317–319 , <i>318–319</i>
computer assignments, 347	capture phase in state migration points, 120
computer associations, 334–336 , 335–337	catalogs in Asset Intelligence, 352–355

categories	branding, 164
configuration items, 431	configuration settings, 142, 256–257
programs, 201	DCM, 428 , 429
CCMAdmins property, 152	enabling, 78, 79
CCMAllowSilentReboot property, 153	general settings, 173–175, 174
ccmclean.exe program, 60–61	installation settings, 84
CCMDebugLogging property, 153	planning, 39
CCMEnableLogging property, 153	restart settings, 173, 173
CcmExec.exe program, 159	settings, 38
CCMInstallDir property, 153	Client Information report, 406
CCMLogLevel property, 153	Client Local Time option, 300
CCMLogMaxHistory property, 154	Client Push Installation Wizard, 156, 156
CCMLoxMaxSize property, 154	client status reporting
ccmsetup.exe program, 158	release R2, 25–26 , 129–134 , 131–135
CD-ROM report, 405	for troubleshooting, 518-521, 521
central sites, 38	Client Status Reporting Setup Wizard,
backups, 524–525	130–131, 131
recovering, 533–536 , <i>533–538</i>	Client Status Reporting Wizard, 519
Change Initiation Review SMF, 10–11	Client tab in push installation, 151, 153
Change Management process, 4, 8	client-to-server port configuration, 35
Changing Quadrant in MOF, 7–8	ClientAgents setting, 84
child configuration items, 445–449	clients, 50
children in hierarchies, 68, 68	Active Directory forests, 36
Choose Collection tab, 454, 455	advertising packages to, 465-467, 466
Choose Configuration Items dialog box, 450,	469–472 , 470–473, 477–479, 478–479
451, 453	configuration baselines, 454-455, 455
Choose Mappings page, 347	deployment parameters, 35
Choose Target Collection page, 336, 337	hardware inventor, 52
class security rights	health collections, 129–130
collections, 181	installation, 141
packages, 194	automatic methods, 157-159
classifications	manual methods, 159
software update points, 115, 118, 252–253,	packages for operating system
273, 274	deployment, 310-312, 311-312
software updates, 240, 276, 276	planning, 39
Classifications page	push. See push client installation
software update points, 115, 118, 273, 274	software features, 141–143 , <i>142</i>
software updates, 276, 276	verifying, 159–160 , 160
client access license data, 363–366 , <i>364</i> , <i>366</i>	inventory reports, 391
Client Agent Selection page, 78, 79	log files, 507–508
client agents	MIF storage location, 380
Asset Intelligence, 350	mobile devices
BITS settings, 173–175, 174	deploying, 476–479 , 477–479

health reports, 479–480	Completed Successfully page, 417
installation, 467-472, 469-473	Completing the Import Object Wizard page,
installation verification, 473–476,	134, 135, 520
475–476	compliance for software updates, 247–248
NAP, 489	Compliance report, 404, 407
prerequisites, 51	compmon.log file, 92
requirements, 27–29	component servers, 91–92
software update settings, 257	Component Status messages, 509, 509
troubleshooting, 518–521 , <i>521</i>	computer associations, 334–336 , <i>335–337</i>
virtual application packages, 233	computer client agent. See client agents
ClientSettings.ini file, 467–468	Computer Client Agent Properties dialog box
ClientStatusReporting.msi file, 130, 519	173–175, 173–174, 310, 311
ClientStatusReports.mof file, 132–133, 521	computer images for operating system
cloning reports, 417	deployment
Collect IDMIF files option, 380	capturing, 319–321 , 320–322
Collect NOIDMIF files option, 380	distributing and deploying, 323 , 324
Collected File Properties dialog box, 388, 390	packaging and advertising, 322–323,
Collection Limiting page, 179, 179	322–323
collections, 18	Computers for a Specific Console User report,
advertisements, 216	352
client health, 129–130	
creating, 176	Computers That Recently Used a Specified
deployment templates, 243, 298, 299	Executable report, 350
direct membership, 176–181 , 177–182	ConfigMgr Logs User Off option, 201
interoperability, 50	ConfigMgr PXE Service Point Properties
mobile device clients, 474	dialog box, 337, 337
query-based, 182–185 , 184–186	ConfigMgr Restarts Computer option, 200
software distribution, 171–172	ConfigMgr Status Message Viewer window,
software inventory, 375	510, 510
status reports, 223	ConfigMgrPrereq.log file, 59, 63, 128
Collections report, 406	ConfigMgrSetup.log file, 129
command line	configuration baselines, 425, 431
Installation Prerequisite Checker, 55	clients, 454–455 , <i>455</i>
programs, 200	configuration items for, 453, 453–454
Resource Explorer, 377	initial, 449–450
WSUS 3.0 Administration Console	options, 455
installation, 269	rules, 450–453 , <i>451</i>
comments	configuration items (CIs), 425
advertisements, 215	attributes and permissions, 439-441,
packages, 187	440–441
programs, 200	for baselines, 453 , <i>453</i> – <i>454</i>
software metering rules, 397	child, 445–449
Companies and Products report, 406	completing, 441–442 , 442–443

creating, 429–431 , <i>430</i> , <i>432</i> , 433–435 ,	distribution points, 207, 210
434–436	programs, 205, 207
detection methods, 431 , 433 , <i>433</i>	software updates lists, 297
overview, 426–428	Console Users on a Specific Computer report,
parent, 442–445	352
validating, 436–439 , 437–438	Control Panel for client installation, 159
Configuration Management process, 3–4, 7–8,	Copy Package function, 92
20 Configuration Manager 2007 Toolkit, 516	Copy Package page for distribution points, 207, 208, 317
Configuration Manager Client Upgrade	copying backups to other locations, 525–526
package, 312	COUNT command, 419–420
Configuration Manager overview, 13, 83	Countdown Seconds setting, 443
Active Directory considerations, 34–36	Create A New Deployment Package option,
boundaries, 36	291
console troubleshooting, 517–518	Create A New Task Sequence page, 324, 324,
deployment	339, 340
intelligence gathering, 31–33, 41–42, 41	Create Application Configuration Item
planning, 33–37	Wizard, 430–434, 432–434, 441–442, 442
troubleshooting, 517	Create Compressed Version Of The Source
disaster recovery, 37	Files option, 198
major features, 17–21 , 18	Create Configuration Baseline Wizard,
new features, 21–27	449–450, 450, 453–454, 453–454
resource discovery, 37	Create Direct Membership Rule Wizard,
security, 37	177–180, 178–180
site design, 37–40	Create Package From Definition Wizard
system requirements, 27–31	Device Client Installer, 469–470, 469–470
Configuration Manager Setup Wizard, 128	Device Management Inventory extension,
configuration.mof file	465, 465–466
CAL reports, 364, 364	operating system deployment, 310–313,
hardware inventory, 52, 350, 371 , 381–382 , 382	311–313
modification requirements, 351–352	software distribution, 196–197, 197–198
Configure Automatic Updates option, 258	CreateSQLDevice setting, 84
Configure State Migration page, 327, 327, 341,	Custom Experience Improvement Program
342	Configuration dialog box, 59, 63, 77, 78
Configure The Network page, 325, 326, 340,	custom labels, 354
341	custom reports, 108 , 110 , 408–410 , 408–410
Configure Validation window, 436–439, 438,	Custom Schedule dialog box
445	client push installation discovery, 146–148
Confirm Object Delete dialog box, 398	148–149
Confirmation page	hardware inventory, 379
collections, 181, 183	updates, 190, 190–191
configuration baselines, 453	Custom Severity page, 255–256

settings overview, 245
software downloads, 290
software updates, 303–306 , <i>304–305</i>
templates, 298 deployment
intelligence gathering, 31–33, 41–42, 41
mobile device client software, 467–468,
476–479 , 477–479
operating system. See operating system
deployment (OSD)
pilot, 40
planning, 33–37 , 42–43 , 43
software updates, 244 , 247–249
downloading, 290–295 , 291–295
finding, 285–290 , 286–289
monitoring, 306
templates, 242–243 , 298–302 , 299–302
troubleshooting, 517
Deployment Management report, 407
Deployment Package page
software updates, 290–291, 291
updates lists, 297, 297
deployment packages
mobile device clients, 468–472 , <i>469–473</i>
software updates, 243–244 , 290–291, 291
updates lists, 297, 297
Deployment Re-Evaluation tab, 264
Deployment Schedule page, 305, 305
Deployment Software Updates Wizard, 241
Deployment States report, 407
Deployment Template page, 304, 304
Deployment Template Wizard, 242–243, 255,
298–302, 299–302
DESC keyword, 419–420
descriptions
configuration items, 430–431, 435
deployment packages, 291
Desired Configuration Management (DCM),
425
applications, 426
client agent setting, 428 , 429
configuration baselines. See configuration
baselines

configuration items. See configuration	out-of-band management, 22
items (CIs)	resources, 37
overview, 425–426	Discovery and Inventory Information report,
reports, 404, 456	406
Desired Configuration Management Client	Discovery Data Record (DDR), 145
Agent, 142	Disk report, 405
Destination Folder page	disk space factors for distribution points, 95,
Client Status Reporting Wizard, 130, 519	166–167
ITMU, 280, 281	Display A Notification Message option, 168
site servers, 77, 78	display names for software inventoried
Detection Method page, 431 , 433, 433, 445	products, 375
device drivers, 344–345 , 344–346	Display Reminders According To The Client
Device Management Inventory Extension	Reminder Intervals option, 220
Package, 463–467 , 465	Display screen for reports, 416, 416
Device Management report, 405	Display/Time Settings page, 243, 300, 300
Device Management window, 475, 476, 479,	distmgr.log file, 97
479	distribution
DHCP-based NAP, 485–486 , 485, 495–496 ,	boot image packages, 316-317
496	computer images, 323, 324
DHCP options for PXE, 336	software. See software distribution
direct membership in collections, 176–181,	Distribution Point page, 213–214, 213–214, 292
177–182	292
Directory Services Administration SMF, 9	distribution points, 92–93, 170
Disable MOM Alerts While This Program	branch, 93, 164, 170, 213–214, 214
Runs option, 205	configuring, 206–208 , 207–208
Disable This Program When It Is Advertised	implementing, 96, 96
option, 204	mobile devices, 460–461, 461, 465, 469–472,
DisableCacheOpt property, 154	470–473
DisableSiteOpt property, 154	protected sites as, 93–95, 94
disabling software metering rules, 394–395	requirements, 166–167
disaster recovery, 37, 523	server shares as, 208–210, 209–210
backups, 524–529 , <i>528</i>	servers as, 210–213 , 211–213
central sites, 533–536 , <i>533–538</i>	software requirements, 95
planning, 523–524	space recommendations and scalability,
post-site-repair tasks, 538, 540–542	95
primary sites, 537–538	troubleshooting, 96–97, 97
restores, 529–532	virtual application packages, 233
site resets, 538 , <i>539</i>	Distribution Points page
starting, 532–533	package advertisements, 219, 219, 466, 471,
Disconnect Users From Distribution Points	473
option, 192, 292	task sequences, 328, 329
discovery	Distribution Settings page
client nush installation 145-151 146-150	branch distribution points 93 94

packages, 192-193, 193, 314 Enable Software Updates on Clients option, software updates, 293-294, 294 Distribution Settings For Inventory Tool page, Enable This System As A Protected Site System 282, 282 option, 209 Distribution Settings For Windows Update Enable Wake On LAN option, 217, 305 Agent page, 282-283, 283 enabling Distribution Status for SMS 2003 Clients Asset Intelligence, **362–363**, *363* client agents, 78, 79 report, 407 DMCommonInstaller.ini file, 467–468 Software Metering Client Agent, 394 DMPSetup.log file, 460 software metering rules, 394–395 DMZs (demilitarized zones), 498 Wake on LAN, 171, 215, 217, 305 Do Not Set A Deadline For Software Update encrypting client inventory reports, 391 Installation option, 305 **Energy Star Power Management** Do Not Synchronize from Microsoft Update or Configuration Pack, 456 an Upstream Update Server option, 271 Enforce All Mandatory Deployments option, Download Content From Distribution Point And Run Locally option, 220 enforcement methods in NAP, 482 Download Location page, 294–295, 294, 297 802.1x NAP, **484–485**, *485*, **494–495**, *495* Download Settings page, 243, 301, 301 DHCP, **485–486**, *485*, **495–496**, *496* Download Software Updates From A Location IPsec, **487**, *488*, **497–498**, *498* On The Local Network option, 295 VPN, **486–487**, *486*, **496**, *497* Download Software Updates From The Enforcement phase in software updates, Internet option, 294 306 Download Software Updates Wizard, 253 environment variables in DCM, 434-435 Download Updates Wizard, 241, 243, 290-295, error codes for inventory, 393 291–295, 297 Errors report, 405 downloading software updates, 290-295, Estimated Disk Space setting, 201 291 - 295Evaluation phase in software updates, 306 DPM (Data Protection Manager), 13–14 Event Generation page, 243, 300 Drive Mode settings, 203 Examination Institute for IT (EXIN), 2 drive selection for state migration points, excluding software inventory files, 391 120-121 execmgr.log file, 230, 231 Driver Details page, 344, 345 existing data in transitions, 52 dynamic IT, **12–13** exporting reports, 417, 418 E update synchronization with, 279 802.1x NAP, **484–485**, *485*, **494–495**, *495* extending hardware inventory, 380–384, Enable binary differential replication option, 382-386 191, 291–292 F Enable Hardware Inventory On Clients option, 378 fallback situations, 49 **Enable Software Distribution To Clients** fallback status points, 35, 97-99

Feature Packs, **52**

option, 167

file collection	New Program For Device Wizard, 477, 477
Mobile Device Client Agent, 462, 464	New Site Role Wizard, 96, 96, 315, 489
software inventory, 375 , 388, 389	New Site System Server Wizard, 489
File Collection tab, 388, 389, 462, 464	operating system image, 323, 323
files for software updates, 241	packages, 187, 187–188, 313, 313
Files report, 406	programs, 200–201, 200–201
Final Progress page, 536, 537	PXE service points, 333
Financial Management process, 4–5, 10	Reporting Point roles, 402, 403
finding software updates, 285–290 , 286–289	reports, 414, 414, 420, 422
Finish page	software distribution, 173, 174, 175,
computer associations, 336	228–230, 229
Site Repair Wizard, 536, 538	software inventory, 387, 387
For Deployments Deadlines Within setting,	software metering, 394–396, 395, 397
264	software update points, 251 , 270, 270
Forefront Client Security integration, 26–27	Software Updates Client Agent, 263, 263
forests, Active Directory, 35–36	state migration points, 315
free drive space	task sequences, 328, 329, 343, 343
client requirements, 27	Generate MOM Alert If This Program Fails
server requirements, 30	option, programs, 205
fspMSI.log file, 99	Gilbert, Jeff, 381
full enforcement in NAP, 493, 494	Global Catalog queries, 150
	global roaming
G	Active Directory schema, 34
general CIs, 426–427, 452	Systems Management Server 2003, 48
General report, 405–406	goals
General settings	determining, 31
Advertised Programs Client Agent,	software updates, 249
167–168 , 168	gold image, 138
advertisements, 215, 215, 343, 343	GROUP BY keyword, 419
client push installation, 146, 147, 151, 152	Group Membership setting, 213
collections, 177, 177	Group Policy, 157, 256–258
Computer Client Agent, 256	
configuration items, 434, 444–445	**
dashboards, 423, 423	Н
Deploy Software Updates Wizard, 303,	hard disk configuration, 30–31
304	hardware inventory, 52, 370–371
distribution points, 207–210, 209, 211, 214	configuration.mof file, 371
hardware inventory, 378–379, 379, 385	configuring, 378–380 , <i>379</i>
Heartbeat discovery method, 147, 148	extending, 380–384 , 382–386
Mobile Device Client Agent, 461, 462	file modification requirements report, 351
New Advertisement For Device Wizard,	MIF files, 373–374
477, 478	mobile devices, 462, 464
New Advertisement Wizard, 470, 472	sms_def.mof file, 371–372

Hardware Inventory Client Agent, 142, 350,	distributing and deploying, 323, 324
369	packaging and advertising, 322–323,
Hardware Inventory page, 462, 464	322–323
hardware reports, 359–360 , 405–406 , <i>405–406</i>	implementation timeframe in upgrades, 62
hardware requirements	Import Computer Information page, 347
Asset Intelligence, 355	Import Computer Information Wizard,
clients, 27–28	335–336, 335–337
servers, 29–30	Import Configuration Data Wizard, 456
health registration authorities (HRAs), 498	Import New Driver Wizard, 344–345, 344–346
health reports, 129–130, 479–480	Import Object Wizard, 133, 417, 520
Heartbeat discovery method, 146–147, 148	Import Wizard, 417
Hide All Deployments from End Users option,	importing
264	client status reports, 132–134 , 134–135,
hierarchies	519–520 , <i>521</i>
planning, 39–40 , 70–71	reports, 417 , 418
site relationships, 68–69 , <i>68</i>	update synchronization with, 279
in upgrades, 52	virtual application packages, 233
Hierarchy Maintenance tool, 532, 540–542	in-band management, 22
HINV setting, 84	in-place upgrades, 40, 58–59
hmon.log file, 69, 70	Incident Management process, 2–3, 9
holding sites, 38	Include Members Of Subcollections option,
HRAs (health registration authorities), 498	217
•	Include Updates In Image page, 327, 327, 342,
1	343
Identification tab	Info tab
configuration baselines, 449–450, 450	client status reporting, 132, 133
configuration items, 430–431, 432	ConfigMgr SQL Server, 519
IDMIF files	Information Systems Examination Board
description, 373–374	(ISEB), 2
storage location on clients, 380	Infrastructure Engineering SMF, 10
Ignore Maintenance Windows and Install	Infrastructure role cluster, 6
Immediately at Deadline option, 255 , 305	Install Required Updates on a Schedule option
Ignore Maintenance Windows When Running	257
Program option, 218	Install Software Packages page, 328, 328, 342
IIS (Internet Information Services), 92	Install The ConfigMgr Client page, 326, 326,
Image Capture Wizard, 319–321, 320–321	340–341, 342
Image Destination page, 319, 320	Install The Windows Operating System page,
Image Information page, 319, 321	324, 325, 339, 341
images	InstallAdminUI setting, 83
client installation, 159	installation
operating system deployment	client. See clients
boot image packages, 316–318,319	Client Status Reporting, 519
capturing, 319–321 , 320–322	software update points, 250–251

Installation page, 130, 131	Inventory Collection tab, 387, 388
Installation Mode Selection page, 265, 265, 268,	Inventory Names tab, 389, 390
268	Inventory Rule Reporting Properties dialog
Installation Prerequisite Check page	box, 385, 385
Configuration Manager Setup Wizard, 128	Inventory Tool for Custom Update (ITCU), 259–260
site servers, 81, 82	Inventory Tool for Microsoft Updates (ITMU)
Installation Prerequisite Check Options page,	installing, 280–284 , 280–283
53, 53	monitoring synchronization process,
Installation Prerequisite Checker, 53–55, 54	285
Installation Progress window, 320, 321	site upgrades, 246, 259–260
Installation Settings page, 74–75, 74, 77	Inventory Agent.log file, 392
Installation Source Files page, 87, 88	IPsec NAP, 487 , <i>488</i> , 497–498 , <i>498</i>
Installation Summary page, 128	IT Infrastructure Library (ITIL), 2-6,11-12
InstallprimarySite setting, 83	IT Service Continuity Management process, 5
InstallSecondarySite setting, 83	IT Service Management (ITSM), 1
instance security rights	dynamic IT, 12–13
collections, 181	ITIL, 2 –6
objects, 241	MOF, 6–11 , 12
packages, 194	System Center products, 13–15, 14
reports, 231, 419	IT Service Management Forum (itSMF), 2
Intel Activity Management Technology, 22	ITCU (Inventory Tool for Custom Update),
Interaction dialog box, 466	259–260
Interaction page	ITMU (Inventory Tool for Microsoft Updates
New Advertisement Wizard, 220–221, 221,	installing, 280–284 , 280–283
471, 473	monitoring synchronization process,
task sequences, 329, 330	285
internal dependencies in software distribution,	site upgrades, 246, 259–260
165	
Internet-based settings in software update	J
point, 251	Job Scheduling SMF, 8
Internet Information Services (IIS), 92	
Interval Between User Notification And	L
Disconnection (Minutes) setting, 192	labels in Asset Intelligence, 354
Intranet FQDN setting, 208	Language Selection page, 253
Inventoried Software Titles node, 354	deployment packages, 295, 295
inventory, 17–18, 369–370	software updates, 297
hardware. See hardware inventory	languages
software	packages, 187
collecting, 374–375	software metering rules, 397
configuring, 387–392 , <i>387–390</i>	software update points, 118, 119, 253 , 275,
mobile devices, 462, 463	275
troubleshooting, 392–393	software updates, 276, 277, 295, 295, 297
viewing, 376–377 , 376 , 391–392	support, 38

Languages tab	Make This Package Available On Protected
software update points, 118, 119, 275, 275	Distribution Points When Requested By
software updates, 276, 277	Clients Inside The Protected Boundaries
launching reports, 109	option, 193, 293
LDAP queries, 149–150	Manage phase for SMFs, 11
License Agreement screen	managed object files (MOFs), 69
Client Status Reporting Setup Wizard, 130	Management information format (MIF) files,
Client Status Reporting Wizard, 519	194, 373–374, 380
ITMU, 280, 280	Management Point page, 79, 81
license management reports, 361–362	Management Point setting, 84
linked subcollections, 171	management points
Links Dialog box, 422	Active Directory schema, 35
links to reports, 416, 422	client load, 38
lists for software updates, 242, 295–297,	log files, 507
296–298	mobile devices, 459–460 , <i>460</i>
load balancing	overview, 99–102 , 103
management points, 101	site servers, 79, 81, 84
reporting points, 110	Mandatory Assignments option, 217
load state for USMT packages, 312	manual processes
Local drive on site server option, 192	client installation, 159
Local Roaming Boundaries, 49	software update synchronization, 246
Locate Driver page, 344, 344	manufacturers of packages, 187
locating server locator points, 112	Maximum Allowed Run Time setting, 164,
locations for reporting points, 110	201
LocationServices.Log file, 101	Maximum Custom MIF File Size (KB) setting
log files	379–380
backup process, 527	Maximum Run Time settings, 254–255
client, 507–508	Media Type page, 317, 318
management points, 101-102	membership, collection, 176–181 , 177–182
mobile device clients, 474	Membership Rules page, 177, 178, 181, 181,
point, 507	185, 186
site servers, 505–506	Memory report, 405
software distribution, 230, 231	messages, status, 509–510 , 509–511
Trace32 log viewer, 516, 516	advertisement, 512-513
for troubleshooting, 504–508	package, 514 , 515
Windows event, 352	site, 515–516 , 516
Log Off Action setting, 443	viewer, 227–230 , 227–230
logon script installation, 157–158	web reports for, 511-512
M	metadata in software updates, 240–241 , 276, 279
maintenance plans, 501–504 , <i>502</i>	metering software. <i>See</i> Software Metering
maintenance windows	feature
software distribution, 164	Microsoft Application Virtualization Desktor
software update point, 254–255	Client, 232
3011Wate update point, 204-200	CHEIR, 202

Microsoft Application Virtualization	Device Management Inventory Extension
Management, 25, 135	Package, 463–467 , 465
packages, 231–233	distribution points, 460-461, 461, 465, 465,
software distribution, 165	469–472 , 470–473
Microsoft Application Virtualization Terminal	management points, 459–460 , 460
Services Client, 232	Modem report, 405
Microsoft Deployment Toolkit, 138	MOF. See Microsoft Operations Framework
Microsoft Operations Framework (MOF), 6	(MOF)
Changing Quadrant, 8	MOF File Name page
ITIL expansion, 6–7	client status reporting, 133, 134
OMRs, 10-11	Import Object Wizard, 417, 417, 520
Operating Quadrant, 8–9	MOFs (managed object files), 69
Optimizing Quadrant, 9–10	MOM Maintenance Mode page, 205, 206
process model, 7–8	monitoring
Supporting Quadrant, 9	ITMU synchronization process, 285
Microsoft Software License Terms page, 74, 74,	site processes, 540
128	software distribution status, 221
Microsoft Updates catalog, 246, 260	log files, 230 , 231
MIF Collection tab, 380	reports, 221–227 , 223–226, 231
MIF File Name setting, 194	Status Message Viewer, 227–230,
MIF (Management information format) files,	227–230
194, 373–374, 380	software updates deployment, 306
	MP_Hinv.log file, 392
migration points, 120–122 , <i>120–122</i> , 315–316 , <i>316</i>	/MP switch in client installation, 158
	mpcontrol.log file, 102
migrations, 61	mpMSI.log file, 102
Mixed mode	mpSetup.log file, 102
security, 37, 47	multicasts, 138
site servers, 75, 84	multiple language support, 38
Mobile Device Client Agent, 142, 461–462,	multiple product updates, 240
462–464	
Mobile Device Manager (MDM), 15	N
mobile devices, 20, 459	NAC (network access control), 481
client software on	names
deploying, 476–479 , 477–479	advertisements, 215
installation, 467–472 , 469–473	configuration items, 430
installation verification, 473–476,	distribution points, 208
475–476	packages, 187, 194, 291
clients	programs, 200
advertising packages to, 465-467, 466,	servers, 83
469–472 , 470–473	sites, 39
health reports, 479–480	software inventoried products, 375
requirements, 29	software metering rules, 396–397

namespaces for SIMS providers, 90–91, 92	New Advertisement Wizard, 215, 215,
NAP. See Network Access Protection (NAP)	328–331, 329–330, 470–472, 472–473
NAP Evaluation tab, 255	New Boundary dialog, 143, 144–145
NAP setting, 84	New Collection Wizard, 177-178, 177,
NAP Wizard, 490–491	181–184, 181–183
Native mode	New Dashboard Wizard, 423, 423-424
security, 37, 47	New Distribution Points Wizard, 207–208, 208,
site servers, 75, 84	317, 323
Network Access account, 310, 310–311	New File or Folder Properties window,
network access control (NAC), 481	434–437, 435–437, 440–441, 440
Network Access Protection (NAP), 20, 481	New Package Wizard, 186–196, 187–189,
Active Directory schema, 34–35	192–196, 313–314, 313–314
architecture, 483 , 484	New Program For Device Wizard, 477–478,
configuring, 488–491 , 489	477–478
enforcement methods, 482	New Program Notification Icon Opens Add Or
802.1x NAP, 484–485 , <i>485</i> , 494–495 , <i>495</i>	Remove Programs option, 168
DHCP, 485–486 , <i>485</i> , 495–496 , <i>496</i>	New Program Wizard, 200–205, 200–207
IPsec, 487 , 488, 497–498 , 498	New Report Wizard, 408–410, 408, 410,
VPN, 486–487 , <i>486</i> , 496 , <i>497</i>	414–416, 414, 416, 419
introduction, 481–482	New Site Manager dialog box, 49–50, 50
phasing in, 491–494, 492, 494	New Site Role Wizard
requirements, 482–483	Asset Intelligence, 366, 366
site servers, 84	distribution points, 93, 94, 96–97, 97
software updates, 255	fallback status points, 97–98, 98
system health validator, 123, 489	management points, 102, 103
testing, 262	PXE service points, 104, 332–334, 332–334
Network Access Protection Client Agent, 142	reporting points, 111, 111, 402, 403–404
Network Access Protection report, 406	server locator points, 113, 114
Network Adapter report, 405, 406	software update points, 115–118, 115–119,
Network Administration SMF, 9	251, 269–275, 270, 272–275
network bandwidth	state migration points, 121–122, 121–122
site design, 37–38	system health validator points, 123, 124, 489
software distribution, 170	New Site System Server Share Wizard,
network connectivity, 517	208–211, 209–211 Now Site System Server Wigard, 210, 212
network discovery method, 146–147, 149	New Site System Server Wizard, 210–213,
network information, 32–33	211–213, 489
Network path (UNC name) option, 192	
Network report, 406	New Site System with Software Update Point option, 269
Never Rerun The Advertise Program option,	New Software Metering Rule Wizard, 396–397
218	397
New Advertisement For Device Wizard,	New Task Sequence Wizard, 324–328,
	-
477-479, 478-479	324-328, 339-342, 340-343

New Virtual Application Wizard, 233	client install package, 310–312 , 311–312
NightWatchman utility, 429–430	device drivers, 344–345 , <i>344–346</i>
No Action Required option, 200	enhancements, 25
NOIDMIF files, 380	Network Access account, 310, 310–311
Notification tab, 168–169 , <i>169</i> , 173, 175	reference computer images
NPS Microsoft Management Console snap-in,	capturing, 319–321 , 320–322
482	distributing and deploying, 323, 324
NTFS drives, 154, 166	packaging and advertising, 322–323,
Number Of Retries Before Disconnecting	322–323
Users setting, 192, 292	state migration points, 315–316 , <i>315–316</i>
_	task sequences
0	advertising, 328-331, 329-331
Object Pad page, 536	bare-metal deployment, 339-344,
objects	340–343
vs. settings, 428–429	for capture image, 317–319 , 318–319
software updates, 241–242	developing, 324-328, 324-328
Objects tab	USMT
client status reporting, 133, 134	packages, 312–314 , <i>313–314</i>
configuration items, 433–434, 444	setup, 309–310 , 310
Import Object Wizard, 520	Operating System report, 406
Office of Government Commerce (OGC), 2	operations management overview, 1
OMRs (Operations Management Reviews), 7, 10–11	dynamic IT, 12–13
	ITIL, 2–6
on-demand package distribution, 193 Only When A User Is Logged On option,	MOF, 6–11 , 12
202	System Center products, 13–15, 14
Only When No User Is Logged On option,	Operations Management Reviews (OMRs), 7,
202–203	10–11
Operate phase for SMFs, 11	Operations Manager, 13
Operating Quadrant MOF, 7–9	Operations Review, 11
operating system	Operations role cluster, 6
CIs, 426–427	Optimizing Quadrant MOF, 7, 9-10
client requirements, 28–29	Options settings for site servers, 83
server requirements, 31	Options tab
operating system deployment (OSD), 20,	client status reporting, 132, 132
137–138, 309	ConfigMgr SQL Server, 519
bare metal, 331	ORDER BY keyword, 419–420
computer assignments, 347	Organization Name setting, 256
computer associations, 334–336,	OUs in client push installation, 151
335–337	out-of-band management
PXE service points, 331–334 , 332–334	new features, 22–23
task sequences, 339-344, 340-343	Service Pack 1, 124–125
boot image package, 316–317	overlapping boundaries, 36

P	server locator points, 112
Package Definition page, 196–198, 197, 199,	software updates, 249
312, 312, 465, 465, 469, 470	upgrades, 53–57 , <i>53–54</i>
Package option for programs, 203	Play A Sound option, 168
Package Recovery page, 536, 536	policies
Package Source setting, 291	group, 257–258
packages	NAP, 481
advertisements, 216, 465-467, 466, 469-472,	Policy Polling Interval (Minutes) setting, 256
470-473, 477-479, 478-479	Poll Intervals setting, 461–462
creating from scratch, 185–196 , <i>186–196</i>	Port Settings page, 79, 81
deployment, 243–244	ports
images, 322–323 , 322–323	site servers, 79, 81
mobile device clients, 468–472 , 469–473	WSUS, 271
package definition files, 196–198, 197, 199,	post review phase in SMS upgrades, 57
312, 312, 465, 465, 469, 470	post-site-repair tasks, 538, 540–542
software distribution, 169	posture in NAP, 483
status messages, 514 , <i>515</i>	power control in out-of-band management, 22
status reports, 223	Preferred Sender setting, 193, 293
virtual applications, 231–233	Preinst.exe tool, 532 , 540–542
Packages report, 406	Prerequisite Check page, 128
Parent Site Settings page, 534, 535	Primary Computer Users report, 352
parents	primary site servers, 67
configuration items, 442–445	backing up, 528 , 528
in hierarchies, 68, 68, 534, 535	custom installation, 76–81, 77–82
keys, 83	implementing, 70
ParentSiteCode setting, 83	recovering, 537–538
ParentSiteServer setting, 83	simple installation, 72–75, 73–76
Partner role cluster, 6	unattended installation, 83-85
peer-to-peer authentication, 487	priority
PeerDPAgent.log file, 97	advertisements, 218
Pending state in Asset Intelligence, 356	packages, 193, 293
permissions for configuration items, 439–441,	Priority setting, 218
440–441	Problem Management process, 3, 9
Permissions tab, 439–441, 441	Process Model, 6
Persist Content Client Cache option, 190	Processor Properties node, 354
pilot deployment, 40	Processor report, 406
pilot phase for SMS upgrades, 57	processors
Plan phase in SMFs, 11	client requirements, 27
planning	server requirements, 30
client agents, 39	Product Key page, 75, 76, 77
deployment, 33–37 , 42–43 , 43	ProductID setting, 83
disaster recovery, 523–524	production deployment phase, 57
reporting points, 109–111 , 111	products in updates, 252–253

Products page	R
software update points, 118, 119, 273, 274	R2
software updates, 276, 277	features, 24–27
Program Can Run settings, 202	installing and configuring, 129–134
Program Rerun Behavior setting, 218–219	RADIUS (Remote Authentication Dial In User
Program Restarts Computer option, 200	Service) protocol, 484, 496
programs	RAM
advertisements, 216	client requirements, 27
creating, 198–205 , 200–206	server requirements, 30
software distribution, 169	Recently Used Executables by a Specified Use:
Progress page, 534, 534	report, 351
Progress report, 407	Recently Used Executables by Number of
Properties tab, 384, 385	Computers report, 350
protected distribution points, 49, 93–95, 94, 170	Recently Used Executables by Number of
Provide A Countdown option, 168	Users report, 351
providers	Recently Used Executables on a Specific
in hardware inventory, 381	Computer report, 351
SMS, 90–91 , 92	Reconnect To Distribution Point At Logon
provisioning workstations, 23	option, 203
Proxy Server Settings page, 366	recovery. See disaster recovery
publishers, 194	Recovery Expert Wizard, 532
push client installation, 143	reference computer images
accounts, 143–145 , <i>144–145</i>	capturing, 319–321 , 320–322
attended, 155–157 , <i>156</i>	distributing and deploying, 323 , 324
boundaries, 143 , 144–145	
discovery methods, 145–151 , 146–150	packaging and advertising, 322–323 , 322–323
settings, 151–155	
PXE - Database page, 333, 334	Reference Connection page, 535
PXE - General page, 104, 106, 333, 333	Reference Site Data Recovery page, 536
PXE Service Point Configuration dialog box,	References report, 407
333	Regional roaming, 48–49
PXE service points	Registry
creating, 331–334 , 332–334	64 bit applications, 435
implementing, 104 , 105–106	configuration items, 444
PXESetup.log file, 104, 334	Release Management process, 4, 8
	release R2
Q	features, 24–27
quadrants in MOF, 6–11	installing and configuring, 129–134
quarantine enforcement client (QEC), 482	Release Readiness Review SMF, 11
quarantine in IPsec NAP, 497, 498	Release role cluster, 7
queries, 18	Reminders tab, 257
query-based collections, 182–185 , <i>184–186</i>	Remote Authentication Dial In User Service
Query Rule Properties window, 184, 184	(RADIUS) protocol, 484, 496

remote console for out-of-band management,	SQL commands, 419–422
23	SQL Reporting Services, 26, 135–137,
remote control, 20	136–137
Remote Roaming Boundaries, 49	status messages, 511–512
Remote Tools Client Agent, 142	viewing, 109 , 410 , 411
repair phase in Site Repair Wizard, 531–532	Reports page, 423, 424
RepairWizard.log file, 530	Required Components to Use Administration
Report SQL Statement window, 414, 415	UI page, 268, 268
Report Viewer, 410, 411, 413, 413	Requirements page
reporting mode in NAP, 491 , 492	New Program For Device Wizard, 477, 478
Reporting page for packages, 193–194, 194	programs, 201–202, 202
Reporting Point roles	Requires A Drive Letter option, 203
default reports, 404–408 , 405–407	Requires Specific Drive Letter option, 203
installing, 401–402 , 402–404	rerun functionality for programs, 164
Virtual Web Directory, 404 , 405	Rerun If Failed Previous Attempt option, 219
reporting virtual directories, 108	Rerun If Succeeded On Previous Attempt
reports and reporting points, 21, 105–108, 401	option, 219
Asset Intelligence, 358–362, 404	resets, site, 538 , 539
client inventory, 391	resource discovery, 37
client status, 25–26 , 129–134 , 131–135,	Resource Explorer, 376–377 , <i>376</i>
518–521 , <i>521</i>	Restart Countdown setting, 254
cloning, 417	Restart Settings page
creating and managing, 413-416 , 414-416	deployment templates, 243, 300,301
custom, 108 , 110 , 408–410 , 408–410	software updates, 255
dashboards, 108, 109	Restart tab
DCM, 456	Computer Client Agent, 257
default, 108	software distribution, 173, 173, 175
importing and exporting, 417, 418	restore phase
launching, 109	Site Repair Wizard, 531–532
mobile device clients, 475–476	state migration points, 120
mobile devices client health, 479–480	restoring backups, 529–532
planning, 109–111 , 111	retention policy for state migration points, 120
process, 108	120
Reporting Point roles	Retry Attempts setting, 443
default reports, 404–408 , 405–407	Retry Delay setting, 461–462
installing, 401–402 , 402–404	Retry Interval setting, 443
Virtual Web Directory, 404 , 405	Review/Accept License Terms dialog box, 244
running, 411–413 , 412–413	rights
security, 419–422	collections, 181
software distribution, 221–227 , 223–226,	packages, 194
231	reports, 419
software metering, 350–351	RMT (Role Management Tool), 482
software updates, 261 , 286 , 286–287	roaming, 48–49

roles. See site server roles	software update synchronization, 246, 252
rsetup.log file, 102, 111	278, 278
RT setting, 84	schema for Active Directory, 34–35, 52
rules	SCSI report, 406
collection, 176–180 , <i>178–180</i>	SDI (server and domain isolation), 497
configuration baselines, 431, 450–453, 451	SDKServer setting, 84
software metering	Search Folder Criteria dialog box, 287, 288
adding, 396–398 , 397	search folders, 287–288 , 288
Automatic Rule Generation, 394–395,	Search For Resources page, 177, 178–179
395	Secondary Site Creation Wizard, 86–87, 86
enabling and disabling, 394–395	secondary site servers, 67
Run Another Program First option, 203	backing up, 529
Run Mode settings, 202–203	implementing, 85–87 , 86–88
Run Once For Every User That Logs On	secure key exchange, 35
option, 204	security
Run Once For The Computer option, 204	advertisements, 220
Run Program From The Distribution Point	modes, 47 , 47–48
option, 220	reports, 419–422
Run setting for programs, 200	site, 37 , 47, 84
Run With Administrative Rights option, 202	Security Administration SMF, 8
Run With User's Rights option, 202	Security Management SMF, 9
running reports, 411–413 , 412–413	Security page
Runs With UNC Name option, 203	advertisements, 221
_	collections, 181, 182
S	deployment templates, 298
scalability of distribution points, 95	New Advertisement Wizard, 472
Scallan, Brent, 499–500	packages, 194, 195, 314
Scan Schedule setting, 263–264	reports, 416, 422
scan state for USMT packages, 312	software metering rules, 398
scanning for software update compliance,	software updates lists, 297, 298
259–261	task sequences, 329
Schedule settings	unknown computers, 338, 339
advertisements, 217–218, 218–219	Security Mode page, 77
client push installation discovery, 146–148,	security rights
147	collections, 181
client status reporting, 132, 133	packages, 194
ConfigMgr SQL Server, 519	reports, 419
New Advertisement For Device Wizard,	Security role cluster, 7
478, 479	Select a Package dialog box, 216, 216
New Advertisement Wizard, 471, 472	SELECT command for reports, 419–420
schedules	Select Media Type page
inventory, 377–378	task sequences, 317, 318
software update clients, 257	unknown computers, 338, 338

Select Resources page, 180, 180	Set Source Directory dialog box, 189, 189
Select Source page, 335, 335	Set Source Directory page, 314
Select Update Source page, 266, 266	Set Viewing Period dialog box, 514
Self Update option, 258	Settings Summary page
Sending Priority setting, 193, 293	Administrative Console, 63
sequenced applications, 232	side-by-side upgrades, 59
sequencing process for virtual application, 232	site servers, 80, 82
server and domain isolation (SDI), 497	Settings tab
Server Information report, 406	configuration items, 444–449
Server locator points (SLPs), 112–113,114	mobile device clients, 475, 475
Server Message Block (SMB) protocol, 92	settings vs. objects, 428–429
server shares, 170, 208–210, 209–210	Setup Complete dialog box
servers	client status reporting, 131
as distribution points, 210–213 , 211–213	ITMU, 283, 519
load balancing, 101	Setup Options page, 128
requirements, 29-31	Setup program, 55–56
site. See site servers	Share The Distribution Folder option, 192,
Systems Management Server 2003, 52	292
Service Continuity Management SMF, 10	SHAs (system health agents), 483
Service Delivery process, 2–3	Shred (Multi-user) Computers report, 352
Service Desk function, 2, 9	Shutdown Action setting, 443
Service Level Agreement Review, 11	Shutdown Hour setting, 443
Service-Level Agreements (SLAs), 3	SHVs (system health validators), 483, 484
Service Level Management (SLM) process, 4,	side-by-side upgrades, 40, 59–60
10	Simple Schedule option, 379
Service Management Functions (SMFs), 6-11	Single Computer page, 335, 335
Service Manager, 14	SINV setting, 84
Service Monitoring and Control SMF, 8	site boundaries, 34, 36 , 47–50 , <i>50</i>
Service Pack 1, 124	Site Code setting, 397
Asset Intelligence 1.5 update, 125-127,	Site Identity page, 86–87, 86
125–127	Site Maintenance page, 538, 539
features, 21–24	site maintenance tasks
implementing, 127–128	CAL licensing collection, 365
out-of-band management, 124–125	requirements, 352
release R2, 129–134 , 131–135	site resets, 538, 539
software requirements, 127	for troubleshooting, 502–503
troubleshooting installation, 128–129, 129	Site Management node, 459
Service role cluster, 6	Site Mode page, 75, 75
Service Support process, 2–3	Site Repair Wizard, 530–532
/Service switch in client installation, 158	central sites, 533–536 , <i>533–538</i>
Set A Deadline For Software Update	primary sites, 537–538
Installation option, 305	starting, 532–533
Set Schedule tab. 454	Site Server page, 87, 87

site server roles, 89–90	sites
component servers, 91–92	failure effects, 530–532
distribution points, 92–97 , 94, 96–97	resets, 538 , 539
fallback status points, 97–99, 98	security, 37 , 47 , 47–48, 84
management points, 99–102 , 103	status messages, 515–516 , <i>516</i>
PXE service points, 104 , 105–106	types and relationships, 67-69, 68
reporting points, 105–111 , 106, 109, 111	SiteSecurityMode setting, 84
server locator points, 112–113 , 114	SiteServerSignCert setting, 84
SMS providers, 90–91	64 bit applications, Registry, 435
software update points, 113–118 , 115–119	skpswi.dat file, 391
state health validator points, 122–123 , 123	SLAs (Service-Level Agreements), 3
state migration points, 120–122 , 120–122	SLM (Service Level Management) process, 4,
site servers, 69	10
database, 87–89 , 88–89	slpmsi.log file, 113
log files, 505–506	smexec.log file, 87, 89
names, 83	SMFs (Service Management Functions), 6–11
prerequisites, 71–72	smpmsi.log file, 122
primary, 67	SMS. See Systems Management Server (SMS)
backing up, 528 , 528	2003
custom installation, 76–81, 77–82	sms_def.mof file, 52
implementing, 70	hardware inventory, 350-351, 370-372,
recovering, 537–538	382–384 , <i>383</i>
simple installation, 72–75 , 73–76	modification requirements, 351
unattended installation, 83-85	WMI classes, 392
secondary, 67	SMS Provider Settings page, 79, 80
backing up, 529	SMS Site reports, 406
implementing, 85–87 , 86–88	SMS Trace, 230
settings, 52	SMSAdminUI.log file, 517
software requirements, 70	smsbkup.log file, 524
troubleshooting, 87, 89	SMSCacheDir property, 154
Site Settings tab	SMSCacheFlags property, 154
client status reporting, 131, 131	SMSCacheSize property, 155
ConfigMgr SQL Server, 519	SMSConfigSource property, 155
site servers, 75, 76, 77	smsdbmon.log file, 89
Site Status dashboard, 509, 509	SMSFSPSetup.log file, 99
Site System Installation Account setting,	SMSHTTPPort property, 155
212	SMSInstallDir setting, 83
Site System node, 69, 69–70	SMSNoWINSLookup property, 155
site systems, 39	smsprov.log file, 89, 91–92, 92
Site Type page, 77, 77	SMSPXEImages\$ folder, 334
SiteCode setting, 83	smsreporting.log file, 111
sitecomp.log files, 92	smsreportinginstall.log file, 111, 402
SiteName setting, 83	SMSSetup.log file, 56

SMSSHVSetup.log file, 123	description, 142
SMSSiteCode property, 155	enabling, 394
smssmpsetup.log file, 122	rules, 396, 397
snapshot archiving, 526–527	Software Metering feature, 19, 393
SoftGrid component, 135	maintenance tasks, 398–399
software categories for Asset Intelligence, 353	new features, 393
software distribution, 18–19, 163	overview, 393–394
Advertised Programs Client Agent,	reports, 350–351
167–169 , 168–169	rules
advertisements, 171, 173, 214-221, 215-219,	adding, 396–398 , 397
221	Automatic Rule Generation, 394–395,
collections. See collections	395
distribution points. See distribution points	enabling and disabling, 395-396
internal dependencies, 165	Software Metering Properties dialog box, 395,
mobile devices, 462, 463, 467	395
new features, 163–165	Software Metering report, 407, 407
packages. See packages	software reports, 360–361 , 406
preparing for, 173–175 , <i>173–174</i>	software requirements
process, 175–176	distribution points, 95
programs, 169, 198-205, 200-206	fallback status points, 98
reports, 406	management points, 102
status, 221	PXE service points, 104
log files, 230 , 231	reporting points, 110
reports, 221–227 , 223–226, 231	server locator points, 113
Status Message Viewer, 227–230,	Service Pack 1, 127
227–230	site servers, 70 , 89
virtual application packages, 231–233	SMS providers, 91
Software Distribution page	software update points, 114
Device Management Inventory Extension,	state migration points, 121
467	system health validator points, 123
Mobile Device Client Agent, 462,463	software update point (SUP) role, 239-240, 249
packages, 313	classifications, 252–253
software families for Asset Intelligence, 353	general settings, 251
software features in client installation,	infrastructure, 249–250
141–143 , <i>142</i>	install, 250–251
software inventory	Internet-based settings, 251
collecting, 374–375	languages setting, 253
configuring, 387–392 , <i>387–390</i>	maintenance windows, 254–255
mobile devices, 462, 463	options, 255
Software Inventory Client Agent, 142, 369	overview, 113–118 , 115–119
Software Inventory page, 462, 463	products, 252–253
Software Metering Client Agent	setting up, 269–275 , 270–275
Asset Intelligence, 350–351	summary details, 254

synchronization, 115, 117, 252, 260, 271, 272	update lists, 295–297 , 296–298
testing, 262	Windows Server Update Services 3.0 Server
update files, 253–254	console, 267–269 , 268
Software Update Point tab, 115, 116	installation, 264-267, 265-267
software updates, 19, 237	Software Updates Deployment Evaluation
CIs, 426–427	Cycle action, 257
client settings, 257	Software Updates Scan Cycle action, 257
client support, 280–285 , 280–283	SoH (statement of health) in NAP, 483
compliance, 247–248	sorting reports, 419–420
Computer Client Agent, 256–257	Sound Card report, 406
current system analysis, 258–261	Source Directory page, 198, 199, 312, 313, 465,
deployments, 244, 247–249	466, 469, 471
Deploy Software Updates Wizard,	Source Files page, 198, 198, 469, 470
303–306 , 304–305	/source switch in client installation, 158
packages, 243–244	SP1. See Service Pack 1
templates, 242-243, 298-302, 299-302	Specify a fully qualified domain name (FQDN)
downloading, 290–295 , 291–295	for this site system on the intranet option,
files, 241	208, 269
finding, 285–290 , 286–289	Specify an Internet-based fully qualified
goals, 249	domain name for this site system option,
group policy settings, 257–258	270
home page, 288–290 , 289	Specify Intranet Microsoft Update Service
lists, 242	Location option, 258
metadata, 240–241	SQL for reports
monitoring, 306	commands, 419–422
new features, 237–238	SQL Reporting Services, 26, 135–137,
objects, 241–242	136–137
planning, 249	views, 414, 415
prerequisites, 238–239	SQLServerName setting, 84
process, 244	Start In setting, 200
properties, 255–256	State Message Reporting Cycle (Minutes)
reports, 261 , 286 , 286–287, 407	setting, 256
search folders, 287–288 , 288	State Migration Point page, 315–316, 316
settings and synchronization, 275–279	state migration points
Software Updates Client Agent	configuring, 315–316 , 316
compliance, 247	overview, 120–122 , 120–122
configuring, 262–264 , 263	State Migration report, 407
description, 142, 240	statement of health (SoH) in NAP, 483
settings, 256	Status Message Details dialog box, 228, 228,
synchronization, 245–246 , 275–279 ,	510, 511
276–278	Status Message: Set Viewing Period dialog
templates, 242–243 , 298–302 , 299–302	box, 514, 515
test labs, 261–262	Status Message Viewer, 227–230 , 227–230

status messages, 509–510 , <i>509–511</i>	operating system image, 323
advertisement, 512–513	packages, 194, 195, 198, 199, 314, 469, 471
package, 514 , 515	programs, 205, 206
site, 515–516 , <i>516</i>	PXE service points, 334
viewer, 227–230 , 227–230	Reporting Point roles, 402, 404
web reports for, 511–512	Site Repair Wizard, 536, 536
Status Messages report, 407	site servers, 75
Status of a Specific Advertisement report, 223,	software updates lists, 297
223–226	task sequences, 318, 328–329, 342
status of software distribution, 221	Summary Details page
log files, 230 , 231	fallback status points, 99
reports, 221–227 , 223–226, 231	New Site Role Wizard, 96
Status Message Viewer, 227–230 , 227–230	PXE service points, 104
Status Viewer Options dialog box, 228–230,	reporting points, 111
229–230	Secondary Site Creation Wizard, 87
Storage Folder page, 315, 316	server locator points, 113
Storage Management SMF, 9	software update points, 118
streaming process for virtual application,	state migration points, 122
232–233	system health validator points, 123
subcollections, 171	supersedence, 247
Sugdinis, Chris, 129	Support role cluster, 6
SUM setting, 84	Supporting Quadrant MOF, 7, 9
summarization tasks for software metering,	supporting education (17,7,7)
398	Suppress Display Notifications On Clients
Summarize Client Access License Data task,	option, 300
352	Suppress Program Notifications option, 204
Summarize Client Access License Weekly	supsetup.log file, 118
Usage Data task, 365	SUSSetup.log file, 273
summary details for software update points,	SWM setting, 84
254	Sync Schedule tab
Summary page	software update points, 115, 117
Asset Intelligence, 366	software updates, 278, 278
clients, 312	Sync Source tab, 115, 117
computer associations, 336	synchronization
configuration baselines, 453, 455	Asset Intelligence, 355 , 365–366 , <i>366</i>
configuration items, 441–442, 443, 445	software update points, 115, 117, 252 , 260,
Deploy Software Updates Wizard, 305–306	271, 272
deployment templates, 302	software updates, 245–246 , 275–279 ,
device drivers, 345	276–278
distribution points, 210, 211	Synchronization page, 273, 273
image capture, 320	Synchronization Point Schedule page, 366
Interaction, 466 New Advertisement Wizard, 472	Synchronization Foint Schedule page, 300 Synchronization Source page, 115, 117, 271, 27
rnew Auvernsement Wizdru, 4/2	3y11C111O111ZatiO11 30uffee page, 113, 117, 2/1, 2/

Synchronize from an Upstream Update Server option, 271	Administrative Console, 62–63 in-place, 58–59
Synchronize from Microsoft Update option,	planning, 53–57 , <i>53–54</i>
271	post upgrade considerations, 63
System Administration SMF, 8	side-by-side, 59–60
System Center Essentials (SCE), 15	types, 57–58
System Center Online service, 353	wipe and load, 61–62
System Center products, 13–15, 14	
System Center Updates Publisher, 244	Т
system health agents (SHAs), 483	Task Manager, 159–160, <i>160</i>
system health validator points, 122–123 , <i>123</i> ,	Task Sequence Information page, 324, 325, 339
489	340
system health validators (SHVs), 483, 484	Task Sequence Media Wizard
system requirements, 27–31	capture images, 317–319, 318–319
System Restart Turnaround Time setting, 254	unknown computers, 338–339, 338–339
System Role Selection page	Task Sequence reports, 407
Asset Intelligence, 366	task sequences
distribution points, 210, 210, 212, 212, 214	advertising, 328–331 , 329–331
fall back status points, 98, 98	bare metal, 339–344 , 340–343
management points, 102, 103	capture images, 317–319 , <i>318–319</i>
New Site Role Wizard, 96	developing, 324–328 , 324–328
New Site System Server Wizard, 489	reports, 407
PXE service points, 104, 105, 332, 332	TCG (Trusted Computing Group), 483
reporting points, 111, 111, 402, 403	Team Model, 6
server locator points, 113, 114	Template Name page, 298, 299
software update points, 115, 115	templates, deployment, 242–243 , 298–302 ,
state migration points, 121, 121, 315, 315	299–302
system health validator points, 123, 124	Terminal Server Gateway (TSG), 482
systems management, 15	test labs
Systems Management Server (SMS) 2003,	setting up, 33
45–46	software updates, 261–262
clients, 50–52 , 159–160	test phase (Pilot) in SMS upgrades, 57
collections, 50	/TestDBUpgrade switch, 55–56
deployment template settings, 243, 302, 302	testing
Feature Packs, 52	databases, 55–56
providers, 79, 80, 90-91 , 92	site backups, 528–529
scenarios, 46–47	software update points, 262
site boundaries and supporting roles,	The Package Does Not Contain Any Source
47–50 , <i>50</i>	Files option, 198
site security, 47 , 47–48	third-party tools for hardware inventory,
site servers and settings, 52	383–384 , <i>384–386</i>
software update support, 280–285 , 280–283	This Program Can Run On Any Platform
upgrading from	option, 201–202

This Program Can Run Only On Specific	Updateable state in Asset Intelligence, 356
Platforms option, 202	Updated Prerequisite Components page, 128
This Rule Applies To The Specified Site And	updates
All Its Child Sites option, 397	NAP, 489–491 , 490
Trace32 log viewer, 516, 516	software. See software updates
troubleshooting, 501	Updates tab, 257
backups, 529	Upgrade Assessment reports, 408
clients, 518–521 , <i>521</i>	upgrading from Systems Management Server
component servers, 92	2003
Configuration Manager console, 517–518	Administrative Console, 62–63
Configuration Manager deployment, 517	in-place, 58–59
distribution points, 96–97 , 97	planning, 53–57 , 53–54
fallback status points, 99	post upgrade considerations, 63
inventory, 392–393	side-by-side, 59–60
log files for, 504–508	types, 40, 57–58
maintenance plans for, 501–504 , <i>502</i>	wipe and load, 61–62
management points, 102	Use A Compressed Copy Of The Source
PXE service points, 104	Directory option, 188–189
reporting points, 111	Use another account for installing this site
server locator points, 113	system option, 270
Service Pack 1 installation, 128–129, 129	Use Custom Countdown Notification Length
site database servers, 89	(Minutes) setting, 220
site servers, 87, 89	Use Package Properties For Status MIF
SMS providers, 91	Matching option, 194
software update points, 118	Use The Site Server's Computer Account To
state migration points, 122	Install This Site System option, 212
status messages for, 509–516 , <i>509–511</i> ,	Use These Fields For Status MIF Matching
515–516	option, 194
system health validator points, 123	User-defined state in Asset Intelligence, 356
Troubleshooting report, 407	User Grace Period (in minutes) setting, 293
Trusted Computing Group (TCG), 483	User State Migration Tool (USMT)
TSG (Terminal Server Gateway), 482	documentation, 314
	package creation, 312–314 , 313–314
U	setup, 309–310 , 310
unattended site server installation, 83–85	/UserOnly switch in client installation, 158
Uncategorized state in Asset Intelligence, 356	Users report, 408
unknown computers feature, 337–339 , 337–339	Users That Recently Used a Specified
update files in software update points, 253–254	Executable report, 351
Update Installation tab, 264	UTC time in deployment templates, 300
Update List Wizard, 290, 296–298, 296–298	
update lists for software updates, 242 ,	V
295–297 , 296–298	validating configuration items, 436-439,
Update Repository node, 290	437–438, 444–449

Update Repository node, 290

validation states in Asset Intelligence, 355–356	collections, 177
Validation tab, 436–437, 437, 444–449	Configuration Manager Setup Wizard, 128
validator points, 122–123, 123, 489	Create Package From Definition Wizard,
Verify Site Hierarchy page, 535, 535	310–312, 311, 465, 469, 469
verifying	distribution points, 317
client installation, 159–160 , <i>160</i>	Import Object Wizard, 520
hierarchy information, 535, 535	Installation Prerequisite Checker, 54
mobile device client software installation,	ITMU, 280
473–476 , 475–476	package definition files, 196
versions	Secondary Site Creation Wizard, 86, 86
packages, 187, 194	Site Repair Wizard, 533, 533
software metering rules, 397	When A Client Is Connected Within A Fast
Video Card report, 406	(LAN) Network Boundary option, 220
viewing	When A Scheduled Program Is About To Run
client status reports, 132–134 , 134–135,	option, 168
519–520 , <i>521</i>	When New Advertised Programs Are
inventory information, 376–377, 376,	Available option, 168
391–392	When This Program Is Assigned To A
reports, 109, 410, 411	Computer option, 204
Virtual Web Directory, 404 , 405	Whether Or Not A User Is Logged On option,
virtual application packages, 231–233	202
virtual local area networks (VLANs), 494–495,	wildcards in DCM, 434-435
495	Windows Components Wizard, 71
Virtual Machine Manager (VMM), 14	Windows Deployment Server, 332
virtual machines, 184	Windows Deployment Services (WDS) server
Virtual Web Directory, 404 , 405	role, 104
Volume Shadow Copy Service (VSS), 523	Windows event log settings, 352
VPN NAP, 486–487 , <i>486</i> , 496 , <i>497</i>	Windows Installer page, 205, 205
	Windows Management Instrumentation
W	(WMI), 247
Wake on LAN feature	Windows Server Update Services (WSUS), 19,
description, 21	237–239
enabling, 171, 215, 217, 305	console, 267–269 , 268
report, 408	installing, 264–267 , 265–267
WCM.log file, 273	reporting events, 252
WDS (Windows Deployment Services) server	software update points, 113-114, 250
role, 104	Synchronization Manager, 245
web reports for status messages, 511–512	Windows System Health Agent (WSHA),
Web Site Selection page, 267, 267	483
Web Site tab, 271, 271	Windows Update Agent (WUA), 114, 247
Welcome page	distribution settings, 282–283, 283
Autorun program, 73	event messages, 252
Client Status Reporting Wizard, 519	software updates clients, 257

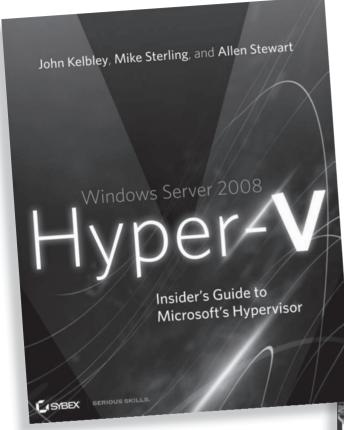
Windows Vista report, 408
Windows XP report, 408
WINS
management points in, 101
server locator points in, 112–113
wipe and load upgrades, 61–62
Wizard Completed screen
dashboards, 423
distribution points, 317
operating system image, 323
packages, 195, 196
reports, 416
task sequences, 318
Workforce Management SMF, 9

WSHA (Windows System Health Agent), 483
WSUS. See Windows Server Update Services (WSUS)
wsusctrl.log file, 118
WSUSUTIL tool, 279
wsyncmgr.log file, 118
WUA (Windows Update Agent), 114, 247
distribution settings, 282–283, 283
event messages, 252
software updates clients, 257

Z

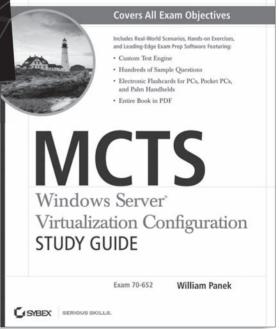
Z28MP01 management point, 159

Your guides to Hyper-V.



Get expert guidance from members of the Microsoft Hyper-V team.

Sybex has Hyper-V certification covered, too.



For more information about these books, go to www.sybex.com/go/virtualization.



Centralize Management of Your IT Infrastructure with SCCM 2007 R2

Deploy software, roll out patches and updates, and track every version of hardware, software, processes, or procedures within your IT infrastructure or enterprise network with the powerful Microsoft System Center Configuration Manager 2007 R2 (SCCM) and the step-by-step instruction in this comprehensive guide.

If you're a systems administrator or IT manager handling a complex Windows Server network, this book is a must. It details all aspects of SCCM 2007 R2, including planning and installation, upgrading, handling security, automating and customizing with scripts, troubleshooting, and much more. Real-world scenarios show you how to apply what you're learning in a variety of contexts—and you'll find pages of useful techniques and tactics to help you master this important, complex tool.

COVERAGE INCLUDES:

- Understanding systems and operations management
- Planning a configuration manager infrastructure
- \bullet Reviewing interoperability with Systems Manager Server 2003
- Distributing, deploying, and updating software
- Managing mobile devices and setting up network access protection
- · Monitoring inventory, software metering, and reporting
- Troubleshooting utilities and preparing for disaster recovery

Centrally Manage Large Groups of Computer Systems

Control the Configuration of Both Software and Hardware

Streamline Administrative Tasks with Remote Tools

Upgrade from Systems Management Server 2003

Learn in the Context of Real-World Scenarios and Tasks

ABOUT THE AUTHORS

Chris Mosby is a three-time SCCM MVP and one of the first members of myITforum.com, Inc. **Ron Crumbaker**, a four-time SCCM MVP and CTO of myITforum.com, Inc., writes frequently on Microsoft subject areas and presents at Microsoft Management Summit conferences. **Christopher W. Urban**, MCSE and MCT, is a Management Tools Product Specialist for Microsoft.

www.sybex.com

ISBN 978-0-470-17367-1



